PREFEITURA MUNICIPAL DE QUATRO BARRAS
EDITAL DE LICITAÇÃO
MODALIDADE: PREGÃO ELETRÔNICO Nº 77/2026
TIPO:MENOR PREÇO GLOBAL

O **Município de QUATRO BARRAS**, Estado do Paraná, através da Comissão nomeada pelo Decreto nº 11.926/2026, torna público, para o conhecimento dos interessados, que de acordo com a Lei nº 14.133/2021, Lei Complementar Federal nº 123/2006, fará realizar na modalidade de PREGÃO ELETRÔNICO, do tipo **Menor preço global.**

OBJETO: Contratação de empresa especializada para o fornecimento de solução integrada e centralizada de segurança cibernética e gestão segura de identidades, contemplando a disponibilização de ativos de segurança perimetral (FIREWALLS em alta disponibilidade – HA), licenciamento de software para proteção avançada de dispositivos (endpoint protection), solução de autenticação multifator (MFA), bem como o fornecimento de licenças, suporte técnico, garantia e demais serviços necessários à implantação, operação e pleno funcionamento da solução, conforme especificações contidas no Termo de Referências (Anexo 01) e no Estudo Técnico Preliminar (Anexo 02) do referido Edital.
MODALIDADE / TIPO: PREGÃO ELETRÔNICO /. MENOR PREÇO GLOBAL
RECEBIMENTO DAS PROPOSTAS: das 17h00m do dia 18/11/2026 as 08h:29min do dia 03/12/2026
INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: 08h:30min do dia 03/12/2026.
MODO DE DISPUTA: ABERTO E FECHADO
VALOR GLOBAL: R$ 2.635.894,80 (dois milhões seiscentos, trinta e cinco mil, oitocentos e noventa e quatro reais e oitenta centavos)
LOCAL: www.comprasbr.com.br "Acesso Identificado"
Para todas as referências de tempo será observado o horário de Brasília (DF).

1 – DA SOLICITAÇÃO E ANEXOS DO EDITAL
1.1 – Solicitação feita através dos processos nº 17.723/2026, protocolado pela Secretaria Municipal de Administração, Finanças e Planejamento.

1.2 – Integram este Edital os seguintes anexos:

ANEXO 01 – Termo de Referências;
ANEXO 02 – Estudo Técnico Preliminar;
ANEXO 03 – Modelo de proposta de preços;
ANEXO 04 – Modelo de declaração unificada;
ANEXO 05 - Minuta do Contrato;

2 – DO OBJETO
2.1 – Tem por objeto o presente Edital de Pregão Eletrônico a Contratação de empresa especializada para o fornecimento de solução integrada e centralizada de segurança cibernética e gestão segura de identidades, contemplando a disponibilização de ativos de segurança perimetral (FIREWALLS em alta disponibilidade – HA), licenciamento de software para proteção avançada de dispositivos (endpoint protection), solução de autenticação multifator (MFA), bem como o fornecimento de licenças, suporte técnico, garantia e demais serviços necessários à implantação, operação e pleno funcionamento da solução, conforme especificações contidas no Termo de Referências (Anexo 01) e no Estudo Técnico Preliminar (Anexo 02) do referido Edital.
2.2 - A administração pública não é obrigada a contratar, as quantidades são apenas estimadas e a contratação ocorrerá sob demanda e de acordo com a disponibilidade financeira.

3 – DO VALOR GLOBAL
3.1 – O valor global para a presente licitação é de **R$ 2.635.894,80** (dois milhões, seiscentos e trinta e cinco mil, oitocentos e noventa e quatro reais e oitenta centavos).
3.2 – Os valores máximos unitários estão relacionados no Anexo 01.

3.3 – A licitação será realizada em lote único, formados por 07 itens, conforme tabela constante do Termo de Referências (Anexo 01), devendo o licitante oferecer proposta para todos os itens que o compõem,

4 – DAS DISPOSIÇÕES PRELIMINARES

4.1 – O Pregão será realizado exclusivamente por meio da INTERNET, mediante condições de segurança – criptografia e autenticação – em todas as suas fases, através do **Sistema de Pregão Eletrônico do Compras Br, no endereço – www.comprasbr.com.br "Acesso Identificado"**, conforme datas e horários definidos neste Edital.

4.2 – Os trabalhos serão conduzidos pela Pregoeira mediante a inserção e monitoramento dos dados gerados ou transferidos pelos licitantes para a plataforma de pregão eletrônico indicada no item 4.1 deste Edital.

4.3 – Será concedido tratamento favorecido para as microempresas (ME), as empresas de pequeno porte (EPP e para o microempreendedor individual (MEI), nos limites previstos da Lei Complementar nº 123/2006.

5 – DAS CONDIÇÕES DE PARTICIPAÇÃO

5.1 – Poderão participar deste pregão todas as empresas que apresentarem os documentos necessários para o respectivo cadastramento junto ao Sistema de Pregão Eletrônico indicado no item 4.1 deste Edital.

5.2 – Poderão participar desta Licitação qualquer firma individual ou sociedade regularmente estabelecida no País, que:

5.2.1 – Estejam com o credenciamento regular no Sistema COMPRAS BR;

5.2.2 – Atuem no ramo pertinente ao objeto da presente licitação;

5.2.3 – Satisfaçam todas as exigências, especificações e normas contidas neste Edital e seus Anexos, inclusive todas as legislações citadas por estes;

5.3 – A licitante, como condição de participação, deverá assinalar "sim" ou "não", em campo próprio do sistema eletrônico, relativo às seguintes declarações:

5.3.1 – Que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021, em se tratando de licitante enquadrado como microempresa, empresa de pequeno porte ou equiparada;

5.3.1.1 – Toda empresa que assinalar o campo "sim" para esse requisito deverá apresentar declaração da condição para análise da Pregoeira, conforme modelo constante no Anexo 04 do edital.

5.3.1.2 – Nos itens onde a participação é exclusiva para microempresas, empresas de pequeno porte e microempreendedores individuais, a assinalação do campo "não", impedirá o prosseguimento da empresa na disputa dos respectivos itens;

5.3.1.3 – Nos) itens abertos à ampla participação, a assinalação do campo "não" acarretará apenas na perda do direito de usufruir dos benefícios concedidos pela Lei Complementar n° 123/2006.

5.3.2 – Que está ciente e concorda com as condições contidas no Edital e seus anexos;

5.3.3 – Que cumpre os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias; e

5.3.4 – Que correspondam a todas as declarações relacionadas no Anexo 04 deste Edital.

5.3.5 – Que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021, em se tratando de licitante organizado em cooperativa.

5.4 – É vedada a participação:

5.4.1 – Das pessoas indicadas pelo art. 14 da Lei Federal nº 14.133/2021;

5.4.2 – Direta ou indiretamente, de servidor dirigente do Município de Quatro Barras, bem como as empresas cujos sócios, administradores, empregados, controladores sejam servidores da mesma.

5.4.3 – De Sociedades Cooperativas e empresa em forma de consórcios ou grupos de empresas;

6 – DOS ESCLARECIMENTOS E IMPUGNAÇÕES

6.1 – Qualquer pessoa é parte legítima para solicitar esclarecimentos ou impugnar edital de licitação por irregularidade na aplicação da Lei Federal n° 14.133/2021, devendo protocolar ou encaminhar o pedido até 03 (três) dias úteis antes da data fixada para a abertura da sessão pública.

6.2 – Não serão conhecidos os pedidos de esclarecimentos solicitados ou as impugnações apresentadas fora do prazo legal.
6.3 – Os pedidos de esclarecimentos poderão ser enviados ao Departamento de Licitações através do Portal COMPRAS BR ou do e-mail licitacao@quatrobarras.pr.gov.br.
6.3.1 – A pregoeira responderá os pedidos de esclarecimentos no prazo de até 03 (três) dias úteis, contados da data de recebimento do pedido. O prazo de resposta se limitará ao último dia útil anterior à data prevista para a abertura do certame.
6.3.2 – Para prestar os devidos esclarecimentos, a pregoeira poderá requisitar subsídios formais aos responsáveis pela elaboração das condições do edital e anexos.
6.4 – As impugnações poderão ser enviadas ao Departamento de Licitações através do Portal COMPRAS BR ou do e-mail licitacao@quatrobarras.pr.gov.br.
6.4.1 – Compete à pregoeira auxiliado pelo setor técnico responsável pela elaboração das condições do edital e anexos, decidir sobre a impugnação. Deverá a Administração responder a impugnação no prazo de até 03 (três) úteis e o prazo de resposta se limitará ao último dia útil anterior à data prevista para a abertura do certame.
6.5 – As respostas aos pedidos de esclarecimentos e impugnações serão divulgadas no Sistema de Pregão Eletrônico do COMPRAS BR e no Portal da Transparência da Prefeitura Municipal de Quatro Barras (www.quatrobarras.pr.gov.br).
6.6 – Os pedidos de esclarecimentos e as impugnações não suspendem os prazos previstos no certame.
6.6.1 – A concessão de efeito suspensivo é medida excepcional e deverá ser motivada pela pregoeira, nos autos do processo da licitação.
6.6.2 – A concessão de efeito suspensivo poderá ocorrer em virtude da necessidade de análise pormenorizada por parte do setor técnico da secretaria requisitante e/ou departamento jurídico.
6.7 – O presente edital e seus anexos poderão ser alterados pela Administração antes da abertura da licitação, pelo interesse público, por sua iniciativa ou decorrente de provocação de terceiros, atendendo com o estabelecido no art. 55 da lei Federal nº 14.133/2021.
6.8 – Decairá do direito de impugnar os termos do edital de licitação perante a administração aquele que não o fizer na forma prevista acima.

7 – DO CREDENCIAMENTO NO SISTEMA ELETRÔNICO
7.1 – Os interessados deverão cadastrar-se junto no **Sistema de Pregão Eletrônico do COMPRAS BR, no endereço –www.comprasbr.com.br**, por meio da apresentação de documentos necessários para o respectivo registro.
7.1.1 – Ao licitante cadastrado será atribuída chave de identificação e senha, pessoal e intransferível.
7.1.2 – O credenciamento será o registro cadastral do licitante no sistema.
7.1.3 – A chave de identificação e a senha privativa do licitante poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado ou por iniciativa do provedor do sistema.
7.2 – O licitante deverá observar as datas e os horários limites previstos no presente Edital para o credenciamento junto ao provedor do sistema para participação da licitação, bem como o cadastramento e a abertura da proposta, atentando também para a data e horário para início da disputa.
7.3 – A participação do licitante no Pregão Eletrônico se dará por meio de seu operador designado, que declarará, em campo próprio do sistema, pleno conhecimento, aceitação e atendimento às exigências de habilitação previstas no Edital.
7.4 – O acesso do operador ao Pregão Eletrônico, para efeito de encaminhamento de proposta de preço e lances sucessivos de preços, em nome do licitante, somente se dará mediante a prévia definição da senha privativa.
7.5 – É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, assumindo como firmes e verdadeiras suas propostas e seus lances, não cabendo à plataforma eletrônica ou à Prefeitura Municipal de Quatro Barras a responsabilidade por eventuais danos decorrentes de uso indevido das credenciais de acesso e senha, ainda que por terceiros.
7.6 – O credenciamento do licitante e 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 à presente licitação.

7.7 – É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no Sistema Eletrônico do COMPRAS BR e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

8 – DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

8.2 – O registro da proposta deverá ocorrer exclusivamente por meio do sistema eletrônico do COMPRAS BR, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

8.3 – O registro da proposta no sistema eletrônico pressupõe pleno conhecimento, aceitação e atendimento das condições previstas neste Edital.

8.4 – Os licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas, sendo que o Município de Quatro Barras não será, em nenhum caso, responsável por esses custos, independente da condução ou do resultado do processo licitatório.

8.5 – No cadastramento da proposta inicial, o licitante deverá observar e atender às condições de participação no processo estabelecidas item 05 deste Edital.

8.6 – A declaração falsa relativa ao cumprimento de qualquer condição, sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

8.7 – Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, não sendo permitido o encaminhamento após o horário estabelecido. Esta instrução, é válida, igualmente, para a inserção dos documentos de habilitação na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances, e de julgamento.

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

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

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

9 – DO PREENCHIMENTO DA PROPOSTA

9.1 – O licitante deverá cadastrar sua proposta no sistema eletrônico mediante o preenchimento dos seguintes campos:

9.1.1 – Valor unitário e total dos itens ou, quando for o caso, percentual de desconto;

9.1.2 – Marca/Fabricante;

9.1.2.1 – Quando o licitante possuir marca e/ou fabricação própria, ou quando o processo licitatório tratar de prestação de serviços, no ato do preenchimento da proposta no sistema eletrônico, o licitante poderá preencher com a redação “marca própria” ou, quando for o caso, “serviço”, a fim de não identificar a empresa.

9.1.3 – Descrição do objeto, contendo informações que atendam todas as especificações técnicas do Anexo I – Termo de Referência.

9.1.3.1 – Em caso de divergência existente entre as especificações dos itens que compõem o objeto descrito no sistema eletrônico e as especificações constantes no Termo de Referências, prevalecerão as últimas.

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

9.3 – O licitante não poderá oferecer proposta em quantitativo inferior à prevista neste Edital.

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

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

9.6 – A apresentação da proposta implica obrigatoriedade do cumprimento das disposições nela contida, assumindo o proponente o compromisso de executar o objeto licitado em conformidade com todos os termos e condições estabelecidas no Termo de Referências (Anexo 01).

9.6.1 – O prazo de validade da proposta não será inferior a 120 (cento e vinte) dias, a contar da data de sua apresentação.

9.6.2 – Os licitantes devem respeitar os preços máximos estabelecidos neste edital.

9.7 – Somente após a etapa de lances e negociação, a pregoeira convocará o licitante detentor da melhor oferta para que, por meio de funcionalidade disponível no sistema e **no prazo de até 02 (duas) horas contados da sua convocação,** envie a proposta adequada (conforme modelo constante do Anexo 03), acompanhada, quando for o caso, da documentação complementar.

9.7.1 - É facultado à Pregoeira prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

10 – DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

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

10.2 – O sistema disponibilizará campo próprio para troca de mensagens entre a Pregoeira e os licitantes.

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

10.4 – O lance deverá ser ofertado conforme critério de julgamento disposto no preâmbulo deste Edital.

10.5 – Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.

10.6 – O licitante somente poderá oferecer valor inferior ou, quando for o caso, maior percentual de desconto ao último lance por ele ofertado e registrado pelo sistema.

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

10.8 – Será adotado para o envio de lances o modo de disputa **“aberto e fechado”**, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

10.8.1 – A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

10.8.2 – Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de maior desconto e os das ofertas com descontos até 10% (dez por cento) inferiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

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

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

10.8.5 – Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem decrescente de descontos.

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

10.10 – Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance ou, quando for o caso, maior desconto registrado, vedada a identificação do licitante.

10.11 – No caso de desconexão com a(o) Pregoeira(o), no decorrer da etapa competitiva da licitação, o Sistema Eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

10.12 – Quando a desconexão do sistema eletrônico para a(o) Pregoeira(o) persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas

vinte e quatro horas da comunicação do fato pela pregoeira aos participantes, no sítio eletrônico utilizado para divulgação.

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

10.14 – Havendo itens não exclusivos para participação de microempresas e empresas de pequeno porte na licitação, uma vez encerrada a etapa de lances, o sistema identificará em campo próprio no sistema as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

10.14.1 – Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima do valor da proposta de menor preço ou abaixo do maior percentual de desconto serão consideradas empatadas com a primeira colocada.

10.14.2 – A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate em relação à proposta da primeira classificada, no prazo de 05 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

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

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

10.15 – Encerrada a etapa de lances da sessão pública, a pregoeira poderá negociar condições mais vantajosas com o primeiro classificado, após definido o resultado do julgamento.

10.15.1 – 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 ou abaixo do desconto mínimo definido pela Administração.

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

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

10.16– A Pregoeira solicitará ao licitante melhor classificado que, **no prazo de 2 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares.

10.16.1 – É facultado à Pregoeira prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

10.16.2 – Apresentar os documentos complementares à proposta conforme o item 4.1 do Termo de Referência.

10.17 – Após a negociação e o envio da proposta adequada, a Pregoeira iniciará a fase de aceitação e julgamento da proposta.

11 – DA FASE DE JULGAMENTO

11.1 – Nesta fase, a Pregoeira verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante consulta nos seguintes cadastros:

11.1.1 – SICAF;

11.1.2 – Cadastro Nacional mantido pela Controladoria- Geral da União - CGU;

11.1.3 – Cadastro Consolidado de Pessoa Jurídica do Tribunal de Contas da União – TCU;

11.1.4 – Cadastro de restrições ao direito de contratar com a Administração Pública do Tribunal de Contas do Estado do Paraná – TCE/PR.

11.1.5 – Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça – CNJ;

11.2 – A consulta aos cadastros relacionadas no item anterior será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei nº 8.429, de 1992.

11.3 – Caso conste na situação do licitante a existência de Ocorrências Impeditivas Indiretas, a Pregoeira diligenciará para verificar se houve fraude por conta das empresas apontadas no Relatório de ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput)

11.3.1 – A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º)

11.3.2 – O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º)

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

11.4 – Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, a Pregoeira verificará se faz jus ao benefício.

11.5 – Verificadas as condições de participação e de utilização do tratamento favorecido, a(o) Pregoeira(o) examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo ou, quando for o caso, desconto mínimo estipulado para a contratação conforme o Edital e seus anexos.

11.6 – Será desclassificada a proposta vencedora que:

11.6.1 – Contiver vícios insanáveis;

11.6.2 - Não obedecer às especificações técnicas contidas no Anexo 01 - Termo de Referência;

11.6.3 - Apresentar preços/descontos inexequíveis ou permanecerem acima do preço máximo/abaixo do desconto mínimo definido para a contratação;

11.6.4 - Não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

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

11.7 – A Pregoeira poderá realizar diligências para aferir a exequibilidade da proposta ou exigir do licitante que ela seja demonstrada.

11.8 – Erros no preenchimento não constituem motivo para a desclassificação automática da proposta. A proposta poderá ser ajustada pelo licitante, no prazo indicado pela Pregoeira, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

11.8.1 – O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância da proposta.

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

11.10 – PROVA DE CONCEITO CONFORME EXPOSTO NO ITEM 4.3 DO TERMO DE REFERÊNCIA.

12 – DA FASE DE HABILITAÇÃO

12.1 – Os licitantes vencedores de forma OBRIGATÓRIA, **no prazo de até 02 (duas) horas contados da convocação pela Pregoeira**, deverão enviar no Sistema Eletrônico do COMPRAS BR todos os documentos necessários para fins de Habilitação. Os documentos que deverão ser incluídos na plataforma são:

12.1.1 – HABILITAÇÃO JURÍDICA

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

b) Microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual – CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade;

c) Sociedade empresária, sociedade unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada – EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada do documento comprobatório de seus administradores;

d) Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME nº 77, de 18 de março de 2020.
e) Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;
f) Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede e matriz;

12.1.1.1 – Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

12.1.2 – REGULARIDADE FISCAL, SOCIAL E TRABALHISTA

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ);
b) Prova de inscrição no Cadastro de Contribuintes Estadual e/ou Municipal, relativa à sede ou ao domicílio do licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;
c) Certidão Negativa de Débitos ou Positiva com Efeito de Negativa relativa aos Tributos Federais, mediante certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por ela administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradoria-Geral da Fazenda Nacional, dentro do seu prazo de validade;
d) Certidão Negativa ou Positiva com Efeito de Negativa de Tributos Estaduais da sede do licitante, dentro do seu prazo de validade;
e) Certidão Negativa ou Positiva com Efeito de Negativa de Tributos Municipais, da sede do licitante, dentro do seu prazo de validade;
f) Certidão de regularidade de débito para com o Fundo de Garantia por Tempo de Serviço (FGTS), dentro do seu prazo de validade;
g) Certidão Negativa de Débitos Trabalhistas - CNDT ou Positiva de Débitos Trabalhistas com Efeito de Negativa, dentro do seu prazo de validade.

12.1.3 – QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

a) Certidão Negativa de Falência ou Concordata/Recuperação Judicial e Extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, dentro de seu prazo de validade.
a.1) Na hipótese de o licitante estar em recuperação judicial, deve ser apresentado comprovante da homologação/deferimento pelo juízo competente do plano de recuperação judicial/extrajudicial em vigor".

12.1.4– QUALIFICAÇÃO TÉCNICA

a) Para fins de comprovação da qualificação técnica, a licitante classificada em primeiro lugar deverá apresentar os seguintes documentos:

a.1) Qualificação Técnico-Operacional (Atestado da Empresa): Comprovação de aptidão para a prestação dos serviços e fornecimento de bens de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, mediante a apresentação de no mínimo 1 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, em nome da licitante, comprovando a execução satisfatória de contratos contendo os seguintes quantitativos e características mínimas: a) Fornecimento, implantação, configuração e suporte técnico de solução de segurança de perímetro do tipo Next-Generation Firewall (NGFW), operando em arquitetura de Alta Disponibilidade (HIGH AVAILABILITY – HA), em quantidade de no mínimo 1 (um) APPLIANCES; b) Fornecimento, implantação ou gerenciamento de solução de

proteção para estações de trabalho (ENDPOINT PROTECTION – EPP/ZTNA), contemplando quantitativo mínimo de 250 (duzentas e cinquenta) licenças (limitado ao teto legal de até 50%); c) Fornecimento, implantação ou gerenciamento de solução de Autenticação Multifator (MFA), contemplando quantitativo mínimo de 40 (quarenta) usuários (limitado ao teto legal de até 50%).

- Será admitido o somatório de atestados de capacidade técnica executados de forma concomitante ou sucessiva para o atingimento dos quantitativos mínimos exigidos.
- Os atestados deverão ser apresentados em nome da licitante (matriz ou filial), não sendo aceitos atestados emitidos em nome de outras empresas pertencentes ao mesmo grupo econômico.
- Os quantitativos mínimos exigidos neste item observam o limite de 50% (cinquenta por cento) do quantitativo estimado, nos termos do art. 67, § 2º, da Lei nº 14.133/2021, e destinam-se exclusivamente a aferir a aptidão técnica da licitante para executar objeto de complexidade equivalente, não constituindo barreira à participação de empresas de menor porte que comprovem experiência compatível.

a.2) Qualificação Técnico-Profissional: Comprovação de que a licitante dispõe, para a fase de execução e implantação do projeto, de equipe técnica qualificada composta por:

- No mínimo 1 (um) profissional designado como Gerente de Projeto, detentor de certificação em Gestão de Projetos emitida por instituição reconhecida (como PMP/PMI, PRINCE2) ou pós-graduação/MBA em Gestão de Projetos;
- No mínimo 1 (um) profissional Especialista em Cibersegurança, detentor de certificação técnica oficial emitida pelo fabricante da solução de Firewall/NGFW efetivamente ofertada na proposta, ou certificação profissional neutra de reconhecimento internacional em Segurança da Informação (tais como CISSP, CISM, CASP+, CompTIA Security+ ou equivalente).
- A comprovação de vínculo dos profissionais com a licitante poderá ser realizada mediante cópia da Carteira de Trabalho (CTPS), Contrato Social (no caso de sócio/diretor), contrato de prestação de serviços assinado ou declaração formal de contratação futura, acompanhada da anuência do profissional designado, nos termos do Art. 67, § 6º, da Lei Federal nº 14.133/2021.

a.3) Declaração de Pleno Conhecimento: Apresentação de Declaração de Pleno Conhecimento das Condições da Contratação, devidamente assinada pelo representante legal da empresa licitante, atestando que a proponente tomou conhecimento de todas as informações, locais e condições para o cumprimento das obrigações do objeto.

Segue abaixo a minuta dos modelos estruturados em estrita conformidade com o Art. 67, § 6º, e Art. 63, § 3º, da Lei Federal nº 14.133/2021:

MODELO III: DECLARAÇÃO DE INDICAÇÃO DA EQUIPE TÉCNICA E TERMO DE DISPONIBILIDADE FUTURA

(A ser apresentado em papel timbrado da empresa licitante, acompanhado dos certificados e comprovante de vínculo do profissional)

À

Departamento de Licitações do Município de Quatro Barras/PR

Ref.: Pregão Eletrônico nº xx/2026 — Indicação da Equipe Técnica (Item 5.4.2)

Pelo presente instrumento, a empresa [Razão Social da Licitante], inscrita no CNPJ/MF sob o nº [CNPJ], por intermédio de seu representante legal infra-assinado, DECLARA, sob as penas da lei, para fins de atendimento às exigências de Qualificação Técnico-Profissional do edital, que indicará para a fase de execução e implantação do projeto a seguinte equipe técnica qualificada:

1.GERENTE DE PROJETO:

- Nome do Profissional: [Nome Completo]
- CPF: [Número do CPF] | Registro Profissional (se houver): [Nº]
- Qualificação/Certificação: [PMP / MBA em Gestão de Projetos / Equivalente] *(diploma/certificado em anexo)*.

- Tipo de Vínculo: ( ) Sócios/Diretor | ( ) Empregado (CTPS) | ( ) Contrato de Prestação de Serviços | ( ) Compromisso de Contratação Futura.

2.ESPECIALISTA EM CIBERSEGURANÇA:

- Nome do Profissional: [Nome Completo]
- CPF: [Número do CPF] | Registro Profissional (se houver): [Nº]
- Qualificação/Certificação: [Certificação Técnica na Solução de Firewall Ofertada / CISSP / CASP+ / CISM / Equivalente] *(certificado em anexo)*.
- Tipo de Vínculo: ( ) Sócios/Diretor | ( ) Empregado (CTPS) | ( ) Contrato de Prestação de Serviços | ( ) Compromisso de Contratação Futura.

TERMO DE COMPROMISSO E ANUÊNCIA DO PROFISSIONAL
(Em conformidade com o Art. 67, § 6º, da Lei Federal nº 14.133/2021)
Eu, [Nome do Profissional], [Nacionalidade], [Estado Civil], [Profissão], portador(a) da Cédula de Identidade RG nº [RG] e inscrito(a) no CPF/MF sob o nº [CPF], DECLARO e atesto para os devidos fins que autorizo minha indicação na equipe técnica da empresa [Razão Social da Licitante] e confirmo minha total disponibilidade pessoal e técnica para atuar na execução e implantação do objeto do Pregão Eletrônico nº 50/2026 do Município de Quatro Barras/PR, caso a referida empresa sagre-se vencedora do certame.
[Local e Data]
[Nome e Assinatura do Representante Legal da Licitante] [CPF do Representante Legal]
[Nome e Assinatura do Profissional Indicado - Gerente de Projeto] [CPF do Profissional]
[Nome e Assinatura do Profissional Indicado - Especialista em Cibersegurança] [CPF do Profissional]

MODELO IV: DECLARAÇÃO DE PLENO CONHECIMENTO DAS CONDIÇÕES DA CONTRATAÇÃO
(A ser apresentada em papel timbrado da empresa licitante, em substituição à vistoria presencial)
À
PREFEITURA MUNICIPAL DE QUATRO BARRAS / PR
Ref.: Pregão Eletrônico nº XX/2026 (Item 5.4.3)
Pelo presente instrumento, a empresa [Razão Social da Licitante], inscrita no CNPJ/MF sob o nº [CNPJ], com sede no endereço [Endereço Completo], por meio de seu representante legal infra-assinado, DECLARA, sob as penas da Lei e para fins de cumprimento das exigências do Edital do Pregão Eletrônico nº XX/2026, que:
1.Tem PLENO CONHECIMENTO de todas as condições da contratação, dos locais de entrega, do ambiente tecnológico, das especificações técnicas descritas nos Anexos 01 e 02 do Edital e das metas dos Acordos de Nível de Serviço (SLA - SOC 24x7x365) exigidos para a execução do objeto;
2.Recebeu todos os elementos, dados e informações suficientes e necessários para o correto e perfeito dimensionamento da proposta comercial, de preços unitários e globais, assumindo total responsabilidade pela exatidão dos quantitativos e custos;
3.Optou por não realizar a vistoria técnica presencial facultativa (ou atesta que as informações do instrumento convocatório são plenamente exaustivas e suficientes), renunciando a qualquer alegação futura de desconhecimento das condições locais, operacionais ou da infraestrutura do Datacenter Municipal para pleitear aditivos contratuais, reequilíbrios ou alterações nos prazos de execução.

12.1.5 – DECLARAÇÃO PARA OUTRAS COMPROVAÇÕES, em conformidade com o modelo constante do Anexo 04:

12.2 **–** Os licitantes que não apresentarem todos os documentos exigidos para fins de habilitação, ou que os apresentarem incompletos, incorretos, serão considerados inabilitados.
12.3 – O prazo para envio dos documentos de que trata o item 12.1, **de até 02 (duas) horas**, poderá ser prorrogado motivadamente pela Pregoeira a depender das circunstâncias ou, havendo justo motivo, mediante solicitação formal de prorrogação por parte do licitante.
12.3.1 – Em caso de não envio dos documentos no prazo indicado ou expirada eventual prorrogação concedida, a licitante será INABILITADA e sujeitar-se-á às sanções previstas neste Edital.

12.3.2 – Em caso de problemas técnicos ou operacionais que inviabilizem o envio pelo sistema, será admitido o envio dos respectivos documentos para o e-mail licitacao@quatrobarras.pr.gov.br, devendo a Pregoeira nessa hipótese, informar no "chat" a data e o horário do recebimento e disponibilizar o conteúdo para os demais licitantes interessados.
12.4 – Os documentos exigidos, quando não contiverem o prazo de validade expressamente determinado, não poderão ter suas datas de expedição superior a 90 (noventa) dias.
12.4.1 – Excetua-se o documento que, por imposição legal, tenha prazo de vigência indeterminado.
12.5 – As microempresas ou empresas de pequeno porte, assim declaradas para efeito dos benefícios da Lei Complementar nº 123/2006, deverão apresentar toda a documentação exigida para a comprovação de regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição.

12.5.1 – Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, prorrogáveis por igual período, a critério da Administração, que terá início no momento em que o proponente for declarado vencedor, para a regularização da documentação com emissão de certidões negativas ou positivas com efeito de negativas;

12.5.2 – A não regularização da documentação no prazo previsto no subitem 12.3.4.1. implicará na decadência do direito à contratação, sem prejuízo das sanções legais, procedendo-se à convocação dos licitantes remanescentes para, em sessão pública, retomar os atos referentes ao procedimento licitatório.

12.6 – Constatado o cumprimento dos requisitos e condições estabelecidos no Edital, o licitante será habilitado e declarado vencedor do certame.
12.7 – Se o licitante desatender às exigências para a habilitação, a(o) Pregoeira(o), respeitada a ordem de classificação, examinará a oferta subsequente de menor preço ou maior desconto, negociará com o seu autor, decidirá sobre a sua aceitabilidade e, em caso positivo, verificará as condições de habilitação e assim sucessivamente, até a apuração de uma oferta aceitável cujo autor atenda aos requisitos de habilitação, caso em que será declarado vencedor.
12.8 – Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

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

12.8.2 – Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

12.9 – Na análise dos documentos de habilitação, a pregoeira poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.
12.10 – O licitante se responsabiliza pela veracidade e autenticidade dos documentos por ele encaminhados.
12.10.1 – A pregoeira poderá solicitar a documentação física para efeitos de comprovação da habilitação do licitante, caso julgue necessário. A necessidade da apresentação dos documentos originais não-digitais somente será exigida quando houver dúvida razoável em relação à integridade do documento digital ou em razão de motivo devidamente justificado.
12.11 – Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).
12.11.1 – A declaração falsa relativa ao cumprimento dos requisitos de habilitação, poderá sujeitar o licitante às sanções previstas em lei e neste Edital.
12.12 – Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao Edital de licitação, após concluídos todos os procedimentos.
12.13 – Do resultado do julgamento da habilitação caberá recurso na forma definida no presente Edital.

13 – DOS RECURSOS E CONTRARRAZÕES

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

13.2 – Declarado o vencedor, qualquer licitante poderá, no prazo de 30 (trinta) minutos, de forma imediata, em campo próprio do sistema, manifestar sua intenção de recorrer. O licitante deverá motivar sua decisão.
13.3 – Havendo manifestação, caberá à pregoeira verificar a tempestividade e a existência de motivação de intenção de recorrer. Nesta fase, a pregoeira não adentará no mérito recursal, apenas verificará as condições de admissibilidade do recurso.
13.4 – Não será concedido prazo para recursos sobre assuntos meramente protelatórios ou quando não justificada a intenção de interpor o recurso pelo proponente;
13.5 – Admitido o recurso, o recorrente terá, a partir de então, o prazo de até 03 (três) dias úteis para apresentar as razões do recurso, pelo sistema eletrônico. Os demais licitantes ficarão intimados para se desejarem, apresentar suas contrarrazões, no prazo de até 03 (três) dias úteis, contados da data final do prazo do recorrente, assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.
13.6 – A falta de manifestação imediata e motivada do licitante quanto à intenção de recorrer, importará na decadência desse direito, ficando a pregoeira autorizado a adjudicar o objeto ao licitante declarado vencedor, encaminhado para a autoridade superior competente para a homologação do mesmo.
13.7 – A pregoeira poderá reconsiderar ou não a decisão recorrida e, em caso de não reconsideração, os autos serão encaminhados ao Prefeito Municipal para julgamento do recurso, observados os prazos previstos no parágrafo. 2º do art. 165 da Lei 14.133/2021.
13.8 – O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.
13.9 – Decididos os recursos, a autoridade competente fará a homologação do objeto da licitação aos licitantes vencedores.

14 – DA REABERTURA DA SESSÃO PÚBLICA
14.1 – A sessão pública poderá ser reaberta:
14.1.1 – Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.
14.1.2 – Quanto houver erro na aceitação da proposta melhor classificada ou quando o licitante declarado vencedor não assinar o contrato ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1° da Lei Complementar n° 123/2006. Nessas hipóteses, a sessão será reaberta na etapa posterior ao encerramento da fase de lances.
14.2 – Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.
14.3 – A convocação se dará por meio do sistema eletrônico e via e-mail.
14.3.1 – A convocação feita por e-mail dar-se-á a partir de dados obtidos junto à plataforma eletrônica, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

15 – DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO
15.1 - Inexistindo manifestação recursal ou decididos os recursos porventura interpostos e constatada a regularidade dos atos procedimentais, a Pregoeira encaminhará o processo à Autoridade Superior que adjudicará o objeto ao licitante classificado em primeiro lugar e homologará o procedimento licitatório.
15.2 - A homologação do resultado desta licitação não implicará direito à contratação.

16 – DA FORMALIZAÇÃO DO CONTRATO
16.1 – Homologada a licitação pela autoridade competente, a Administração firmará contrato específico com o licitante vencedor visando o fornecimento ou a execução do objeto desta licitação nos termos da minuta do Anexo 05 que integra este Edital.
16.2 – O prazo para assinatura do contrato será no máximo 03 (três) dias úteis, contados da convocação expressa do licitante vencedor.
16.2.1 – Serão aceitas assinaturas digitais.
16.3 – Por ocasião da assinatura do Contrato, será exigida a comprovação das condições de habilitação consignadas neste Edital, que deverão ser mantidas pelo licitante durante toda a vigência do Contrato, em atendimento ao §4º do art. 91 da Lei nº 14.133/2021.

16.4 – Se, por ocasião da formalização do Contrato, a documentação relativa à regularidade fiscal e trabalhista estiver com os prazos de validade vencidos, o Município verificará a situação por meio eletrônico hábil, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por tais meios, salvo impossibilidade devidamente justificada.
16.4.1 – Se não for possível atualizá-las por meio eletrônico hábil de informações, a adjudicatária será notificada para comprovar a situação de regularidade mediante a apresentação da respectiva documentação, com prazos de validade em vigência, sob pena de decair do direito à contratação.
16.5 – Nas hipóteses de o licitante vencedor não comprovar as condições de habilitação consignadas no Edital ou se recursar a assinar o Contrato, dentro do prazo estabelecido, serão convocados os licitantes que aceitarem fornecer os bens, executar a obra ou os serviços, seguindo a ordem de classificação, sem prejuízo da aplicação das penalidades previstas em Edital e na legislação vigente.

17 – DA ALTERAÇÃO DO CONTRATO
17.1 – Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.
17.2 – A CONTRATADA será obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato que se fizerem nas obras, nos serviços ou nas compras, e, no caso de reforma de edifício ou de equipamento, o limite para os acréscimos será de 50% (cinquenta por cento).
17.3 **–** Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

18 – DOS PRAZOS, LOCAL E DAS CONDIÇÕES DA PRESTAÇÃO DOS SERVIÇOS
18.1 **–** O prazo de vigência do contrato será de até 60 (sessenta) meses, contados da assinatura do mesmo, podendo ser prorrogado na forma dos Artigos 106 e 107 da Lei nº 14.133, de 2021.
18.2 – O prazo para assinatura do contrato será no máximo de 03 (três) dias úteis a contar da convocação expressa do licitante vencedor, observadas as condições dispostas nos itens 16.3, 16.4 e 16.5 do edital.
18.3 – **O prazo de execução dos serviços será:**
A execução das etapas do objeto dar-se-á nos seguintes prazos, contados a partir do dia útil seguinte ao recebimento da Nota de Empenho, Ordem de Serviço ou documento equivalente:

- Até 30 (trinta) dias úteis para a entrega física de todos os ativos de hardware no Datacenter, montagem em rack, cabeamento, migração completa da matriz de regras de rede, ativação em massa das subscrições lógicas (EPP, ZTNA, MFA e PAM) e homologação do ambiente com a entrega do relatório técnico As BUILT.
- Até 45 (quarenta e cinco) dias úteis para a conclusão e entrega do Serviço de Transferência de Conhecimento (Treinamento Técnico Oficial com carga horária mínima de 24 horas e fornecimento dos vouchers de certificação) para a equipe da Diretoria de TIC.
- 60 (sessenta) meses consecutivos para a prestação dos serviços continuados de suporte técnico, atualizações dinâmicas de segurança e monitoramento proativo via Centro de Operações de Segurança (SOC 24x7x365), contados a partir da assinatura do Termo de Recebimento Definitivo da implantação inicial.

18.4 – **Local, horário e endereço de entrega**
Local de Entrega e Ativação Lógica: Os ativos físicos deverão ser entregues e instalados diretamente no Datacenter Central do Município, e as configurações/ativações lógicas deverão cobrir todos os computadores, servidores e usuários conectados à rede corporativa da Prefeitura Municipal de Quatro Barras/PR.
Endereço Completo: Prefeitura Municipal de Quatro Barras, Av. Dom Pedro II, nº 110 – Centro – Quatro Barras – PR, CEP 83.420-000.
Horário de Recebimento: Os bens físicos e as equipes técnicas da CONTRATADA para a instalação presencial serão recebidos exclusivamente em dias úteis, de segunda a sexta-feira, das 08h00 às 12h00 e das 13h30 às 16h30, mediante prévio agendamento com a fiscalização do contrato.
Nota Operacional: A janela de virada de chave e homologação final dos FIREWALLS poderá ocorrer fora do expediente tradicional (finais de semana ou madrugadas) para evitar a paralisação dos

serviços públicos essenciais (saúde, arrecadação, segurança), desde que previamente acordada e autorizada pelo Departamento de TI.
18.5 – Os serviços ao serem executados deverão estar em conformidade com o solicitado em edital e Termo de Referências (Anexo 01). O recebimento será feito na forma determinada pelo Decreto Municipal n° 11.925/2026.
18.6 – Demais condições da execução dos serviços estão descritas no Anexo 01 (Termo de Referência) do referido edital.

19 – DA FORMA DE PAGAMENTO
19.1 – Deverão ser apresentadas as notas fiscais/faturamentos nas dependências da secretaria municipal solicitante, devendo conter no corpo da nota fiscal as informações a seguir:
a) Descrição dos serviços, o número do empenho, banco, a agência bancária e o número da conta corrente para depósito do pagamento;
b) Juntamente com a nota fiscal, deverão ser apresentadas as cópias dos seguintes documentos de suporte:
b.1) certidão Negativa de Débito – CND do Instituto Nacional de Seguridade Social conjunta com a Certidão Federal - PGFN;
b.2) certificado de Regularidade do FGTS;
b.3) certificado de Regularidade dos Débitos Trabalhistas (CNDT);
b.4) certificado de Regularidade do Município (do Município sede do licitante);
b.5) cópia do empenho encaminhado para a empresa para agilizar o recebimento.
c) O prazo para o pagamento será de 30 (trinta) dias úteis em conformidade com os Decretos Municipais 9.469/2023 e 10.279/2024.
d) Quando a documentação para cobrança estiver incompleta e/ou apresentar elementos que a invalide, deverá ser substituída pela licitante, dispondo a PREFEITURA de 08 (oito) dias corridos a partir do recebimento da documentação correta, para análise e pagamento.
e) O CNPJ do estabelecimento que participar do certame, matriz/sede ou filial, deverá ser o mesmo a constar no Contrato e nas Notas Fiscais/Faturas emitidas, quando da execução dos serviços contratados. Dessa forma, não será admitida a emissão de Notas Fiscais/Faturas por CNPJ de estabelecimento diverso daquele participante da Licitação.
f) Será efetuado retenção tributária prevista na legislação aplicável.

20 – DOS RECURSOS FINANCEIROS
20.1 – Os recursos financeiros para o pagamento de despesas correrão por conta da dotação orçamentária:

Órgão	Código Reduzido	Subação	Natureza	Fonte
03.001	20	03001041220002200833904000000	Serviços de TIC – PJ	1000 – Recurso livre
03.003	56	03003041260025221133904000000	Serviços de TIC – PJ	1000 – Recurso livre
04.003	151	04003219000080244003433390400000	Serviços de TIC – PJ	1000 – Recurso livre
06.001	223	06001103010012207633904000000	Serviços de TIC – PJ	1303 – Recurso livre
25.002	566	25002123650018203933904000000	Serviços de TIC – PJ	1103 - Recurso livre
25.002	567	2500212365001820393390400000	Serviços de TIC – PJ	1104 - Recurso livre
25.003	598	25003123610017203933904000000	Serviços de TIC – PJ	1103 - Recurso livre

21 – DA EXECUÇÃO E DA FISCALIZAÇÃO DO CONTRATO
21.1 – Caberá aos fiscais e aos gestores de Contrato, designados pela autoridade competente por meio do Decreto Municipal nº 11.924/2026, acompanhar e fiscalizar o cumprimento das obrigações contratuais e promover todas as ações necessárias ao fiel cumprimento do Contrato.

22 – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS
22.1 – Comete infração administrativa a empresa e/ou a Contratada que cometer quaisquer das infrações previstas no art. 155 da Lei n°14.133/2021, quais sejam:

1 – Dar causa à inexecução parcial do Contrato;

2 – Dar causa à inexecução parcial do Contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
3 - Dar causa à inexecução total do Contrato;
4 – Deixar de entregar a documentação exigida para o certame;
5 – Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
6 – Não celebrar o Contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
7 – Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
8 – Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante o certame ou a execução do Contrato;
9 – Fraudar o processo ou praticar ato fraudulento na execução do Contrato;
10 – Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
a) Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quando ao enquadramento como ME/EPP ou o conluio entre os prestadores de serviço, em qualquer momento do processo, mesmo após o encerramento da fase de lances;
11 – Praticar atos ilícitos com vistas a frustrar os objetivos do certame;
12 – Praticar ato lesivo previsto no art. 5° da Lei n° 12.846/2013.

22.2 – Serão aplicadas ao responsável pelas infrações administrativas previstas na Lei as seguintes sanções:

a) Advertência, quando a contratada der causa à inexecução parcial do Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2°, da Lei);

b) Impedimento de licitar e contratar, quando praticadas as condutas descritas nos subitens 2 a 7 do item 22.1, sempre que não se justificar a imposição de penalidade mais grave (art. 156 §4°, da Lei);

c) Declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública Direta e Indireta do Ente Federativo que tiver aplicado a sanção, quando praticadas as condutas descritas nos subitens 8 a 12, bem como nos subitens 2 a 7 que justifiquem a imposição de penalidade mais grave (art. 156, §5, da Lei).

d) Multa:

d.1 – moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

d.1.1 – o atraso superior a 30 (trinta) dias autoriza a Administração a promover a rescisão do Contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme o disposto no inciso I, do art. 137, da Lei nº 14.133/2021.

d.2 – moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor total do Contrato, até o máximo de 30% (trinta por cento) pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;

d.3 – compensatória de 30% (trinta por cento) sobre o valor total do Contrato, no caso de inexecução do objeto.

22.3 – A aplicação das sanções previstas não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art.156, § 9º).
22.4 – Todas as sanções previstas poderão ser aplicadas cumulativamente com a multa (art. 156, § 7º);

1 – Antes da aplicação da multa, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contados da data de sua intimação (art. 157);

2 – Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante a Contratada, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, § 8º);

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

22.5 – A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133/2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar e contratar.
§ 1º - Na aplicação das sanções serão considerados (art. 156 §1°):

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 a Administração Pública;
e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

22.6 – Os atos previstos como infrações administrativas na Lei n° 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 1º de agosto de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei (art. 159).

22.7 – A personalidade jurídica da contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos nesta Lei 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, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160).

22.8 – Os órgãos e entidades dos Poderes Executivo, Legislativo e Judiciário de todos os entes federativos deverão, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por eles 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)

22.9 – 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 14.133/2021.

23 – DAS DISPOSIÇÕES FINAIS

23.1 – A presente licitação, não importa necessariamente em contratação, pode o promotor revogá-la, no todo ou em parte, por razões de interesse público, derivada de fato superveniente comprovado ou anulá-la por ilegalidade, de ofício ou por provocação mediante ato escrito e fundamentado. O promotor poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas ou para sua abertura.

23.2 – O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato, sem prejuízo das demais sanções cabíveis.

23.3 – É facultado à pregoeira ou à autoridade a ela/ele superior, em qualquer fase da licitação, promover diligências com vistas a esclarecer ou a complementar a instrução do processo.

23.4 – Os proponentes intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pela pregoeira, sob pena de desclassificação/inabilitação.

23.5 – O desatendimento de exigências formais não essenciais não importará no afastamento do proponente, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

23.6 – As normas que disciplinam este Pregão Eletrônico serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

23.7 – A íntegra do Edital será divulgada no Portal www.COMPRAS BR.org.br, Portal Nacional de Contratações Públicas – PNCP e no site <https://quatrobarras.pr.gov.br/home.php>, na aba licitações.

23.8 – O extrato do Aviso de Licitação será divulgado no Diário Oficial do Município e diário de grande circulação.

23.9 – Os casos não previstos neste Edital serão decididos pela pregoeira.

23.10 – A participação do proponente nesta licitação implica em aceitação de todos os termos deste Edital.

23.11 – Não cabe à plataforma eletrônica qualquer responsabilidade pelas obrigações assumidas pelo licitante com o licitador, em especial com relação à forma e às condições da prestação de serviços e quanto à quitação financeira da negociação realizada.

23.12 – O foro designado para julgamento de quaisquer questões judiciais resultantes deste Edital será **da Comarca de QUATRO BARRAS**, considerado aquele a que está vinculado a(ao) pregoeira(o).
23.13 – A pregoeira e sua Equipe de Apoio, atenderá aos interessados no horário compreendido das 8h00 às 12h00 e das 13h30 às 17h30, de segunda a sexta-feira, no Endereço Av. D. Pedro II, nº 110 – Centro, ou telefone (41) 3671-8800 ou e-mail licitacao@quatrobarras.pr.gov.br, para melhores esclarecimentos.
23.14 – A documentação apresentada para fins de habilitação da empresa vencedora fará parte dos autos da licitação.
23.15 – Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subseqüente, no mesmo horário e local anteriormente estabelecidos, desde que não haja comunicação da pregoeira em contrário.

QUATRO BARRAS, 17 DE NOVEBRO DE 2026.

Atenciosamente,

APARECIDA ALVES DE PAULA SBRISSIA
Pregoeira Municipal

ANEXO 01
TERMO DE REFERÊNCIAS

OBJETO: O presente Pregão Eletrônico tem por objeto a Contratação de empresa especializada para o fornecimento de solução integrada e centralizada de segurança cibernética e gestão segura de identidades, contemplando a disponibilização de ativos de segurança perimetral (FIREWALLS em alta disponibilidade – HA), licenciamento de software para proteção avançada de dispositivos (endpoint protection), solução de autenticação multifator (MFA), bem como o fornecimento de licenças, suporte técnico, garantia e demais serviços necessários à implantação, operação e pleno funcionamento da solução,

1. – ESPECIFICAÇÕES DOS SERVIÇOS / PREÇO ESTIMADO:
1.1 – Em caso de divergência existente entre as especificações dos itens que compõem o objeto descrito no sistema eletrônico e as especificações constantes neste Termo de Referências, prevalecerão as últimas.

Valor total máximo de contratação: **R$ 2.635.894,80** (dois milhões, seiscentos e trinta e cinco mil, oitocentos e noventa e quatro reais e oitenta centavos).

Item	Descrição	Qtd p/ 60 meses	Und	Valor máximo unitário	Valor máximo Total p/ 60 meses
1	Firewall para Segurança de Rede: Fornecimento de Appliance (HARDWARE + SOFTWARE) em modo cluster (alta disponibilidade ativo-passivo), com THROUGHPUT mínimo de 26 GBPS (Firewall) e 35 GBPS (VPN). Formato RACK (máx. 1U). Deve incluir suporte a SD-WAN, filtro de conteúdo, IPS, antivírus de gateway, AntiSpam e Licenciamento de subscrições para o período contratual. Demais informações técnicas, estão no item 11 deste termo.	120	Und	**R$ 8.041,10**	**R$ 964.932,00**
2	Armazenamento de Logs: Fornecimento em máquina virtual. Centralização de logs e geração de relatórios com coleta mínima de 25gb logs diários e licenciamento de subscrições para o período contratual. Demais informações técnicas, estão no item 11 deste termo.	60	Und	**R$ 3.319,91**	**R$ 199.194,60**
3	Proteção Avançada para estações, composta com EPP e ZTNA, com suporte para menos os seguintes sistemas operacionais: WINDOWS, LINUX E MACOS. Licenciamento de subscrições para o período contratual. Demais informações técnicas, estão no item 11 deste termo.	36000	Licença	**R$ 18,90**	**R$ 680.400,00**
4	Proteção Avançada para Gestão Segura de Identidade: AUTHENTICATOR com 100 Licenças de uso de software de autenticação multifator (MFA), em conformidade com a LGPD, com suporte a 10 soft tokens móveis (PUSH, QR CODE, OTP), portal Single SIGN-ON (SSO), sincronismo nativo com AD/LDAP. Licenciamento de subscrições para o período contratual. Demais informações técnicas,	60	Und	**R$ 1.791,15**	**R$ 107.469,00**

	estão no item 11 deste termo.				
5	Solução de Acesso Privilegiado (PAM): Software para segurança para gerenciamento, controle e monitoramento das Contas com acesso privilegiado aos servidores de missão crítica. Licenciamento de subscrições para o período contratual. Demais informações técnicas, estão no item 11 deste termo.	300	Serv	**R$ 533,98**	**R$ 160.194,00**
6	Treinamento: Serviço de capacitação técnica para até 10 profissionais indicados (e até 3 ouvintes), com carga horária mínima de 24 horas, incluindo fornecimento de Material didático oficial e emissão de certificados oficiais. Demais informações técnicas, estão no item 11 deste termo. Deverá ser fornecido 4 vouchers para certificação oficial do fabricante (nível inicial)	300	Serv	**R$ 465,47**	**R$ 139.641,00**
7	Implantação: Serviço de instalação física, cabeamento, configuração, ativação e migração integral de regras/políticas vigentes na rede municipal. O prazo de execução é de até 30 dias, com posterior entrega de documentação "as BUILT" editável. Demais informações técnicas, estão no item 11 deste termo.	540	Serv	**R$ 711,23**	**R$ 384.064,20**

1.1.1. Descrições detalhadas dos itens:

CARACTERÍSTICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW): Deverá possuir no máximo 1 RU de altura; Deve suportar, no mínimo, 26 (vinte e seis) GBPS de THROUGHPUT com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote; Deve suportar, no mínimo, 11 (onze) milhões de conexões simultâneas; Deve suportar, no mínimo, 400.000 (quatrocentas mil) novas conexões por segundo; Deve Suportar, no mínimo, 35 (trinta e cinco) GBPS de THROUGHPUT VPN IPSEC; Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC SITE-TO-SITE simultâneos; Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 16.000 (dezesseis) túneis de clientes VPN IPSEC simultâneos; Deve suportar, no mínimo, 03 (três) GBPS de THROUGHPUT de VPN SSL; Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos; Deve suportar, no mínimo, 09 (nove) GBPS de THROUGHPUT de IPS; Deve suportar, no mínimo, 07 (sete) GBPS de THROUGHPUT de Inspeção SSL; Deve suportar, no mínimo, 06 (seis) GBPS de THROUGHPUT com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e ANTIMALWARE. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45; Deve possuir, pelo menos, 8 (oito) interfaces MULTI-GIGABIT Ethernet 5 GBPS BASE-T com conectores RJ-45; Deve possuir, pelo menos, 4 (quatro) interfaces Gigabit Ethernet com conectores SFP; Deve possuir, pelo menos, 8 (oito) interfaces 10 Gigabit Ethernet com conectores SFP+; Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento; Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade; Deverá possuir interface USB; Deve estar licenciado para gerenciar até 64 (sessenta e quatro) switches e 256 (duzentos e cinquenta) pontos de acesso sem fio simultaneamente em um único APPLIANCE; Deve possuir fonte de alimentação AC redundante; Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por APPLIANCE; Os equipamentos devem ser entregues com todas as funcionalidades descritas neste termo de referência licenciadas e disponível para uso, além de suporte e garantia por todo o tempo de contrato (60 meses).

Características gerais para os equipamentos NGFW: A solução deve consistir em plataforma de proteção de rede baseada em APPLIANCE físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open SOURCE (produto montado); Por

funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões; A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta; Os dispositivos de proteção de rede devem possuir suporte a VLANS; Os dispositivos de proteção de rede devem possuir suporte a roteamento MULTICAST (PIM-SM e PIM-DM); Deve suportar BGP, OSPF, RIP e roteamento estático; Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay; Os dispositivos de proteção de rede devem possuir suporte a DHCP Server; Os dispositivos de proteção de rede devem suportar SUB-INTERFACES ethernet logicas; Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall; Deve suportar NAT dinâmico (MANY-TO-MANY); Deve suportar NAT estático (1-to-1); Deve suportar NAT estático bidirecional 1-to-1; Deve suportar Tradução de porta (PAT); Deve suportar NAT de Origem; Deve suportar NAT de Destino; Deve suportar NAT de Origem e NAT de Destino simultaneamente; Deve implementar Network PREFIX TRANSLATION (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico; Deve suportar NAT64; Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança; Enviar log para sistemas de monitoração externos; Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL; Proteção ANTI-SPOOFING; Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego; Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo; A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB; O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link; Controle, inspeção e de criptografia de SSL para tráfego de Saída (OUTBOUND); A solução deve suportar integração nativa com LET'S ENCRYPT, para obtenção de certificados válidos, de forma automática; Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos; os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de END-OF-LIFE e END-OF-SALE; A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e KUBERNETES; deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via TEAMS e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos; Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de COMPLIANCE na VPN; Deverá suportar controles por zonas de segurança; Deverá suportar controles de políticas por porta e protocolo; Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações; Controle de políticas por usuários, grupos de usuários, IPS, redes e zonas de segurança; Controle de políticas por código de País (Por exemplo: BR, US, UK, RU); Controle, inspeção e descriptografia de SSL por política para tráfego de saída (OUTBOUND); Deve decriptografar tráfego OUTBOUND em conexões negociadas com TLS 1.2 e TLS Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada; Suporte a objetos e regras IPV6; Suporte a objetos e regras MULTICAST; Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

Controle de Aplicações: Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo; Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos; Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a PEER-TO-PEER, redes sociais, acesso remoto, update de software, protocolos de rede, VOIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail; Deve inspecionar o PAYLOAD de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo; Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor; Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de PAYLOAD para checagem de assinaturas de aplicações conhecidas pelo fabricante; Deve realizar decodificação de protocolos com

o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação; Identificar o uso de táticas evasivas via comunicações criptografadas; Atualizar a base de assinaturas de aplicações automaticamente; Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active DIRECTORY, sem a necessidade de instalação de agente no Domain CONTROLLER, nem nas estações dos usuários; Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras; Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos; Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante; O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; Deve alertar o usuário quando uma aplicação for bloqueada; Deve possibilitar a diferenciação de tráfegos Peer2Peer (BITTORRENT, emule, ETC) possuindo granularidade de controle/políticas para os mesmos; Deve possibilitar a diferenciação de tráfegos de INSTANT MESSAGING (AIM, HANGOUTS, Facebook Chat, ETC) possuindo granularidade de controle/políticas para os mesmos; Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD; Deve possibilitar a diferenciação de aplicações Proxies (PSIPHON, FREEGATE, ETC) possuindo granularidade de controle/políticas para os mesmos; Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (CLIENT-SERVER, BROWSE BASED, Network PROTOCOL, ETC); Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade; Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação; Deve permitir forçar o uso de portas específicas para determinadas aplicações; Deve permitir o filtro de vídeos que podem ser visualizados no YouTube; Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e ANTI-SPYWARE integrados no próprio APPLIANCE de firewall; Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e ANTI-SPYWARE); Deve sincronizar as assinaturas de IPS, Antivírus, ANTI-SPYWARE quando implementado em alta disponibilidade; Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo; As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração; Deve ser possível a criação de políticas por usuários, grupos de usuários, IPS, redes ou zonas de segurança; Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura; Deve suportar granularidade nas políticas de IPS, Antivírus e ANTI-SPYWARE, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens; Deve permitir o bloqueio de vulnerabilidades; Deve permitir o bloqueio de EXPLOITS conhecidos; Deve incluir proteção contra-ataques de negação de serviços; Ser imune e capaz de impedir ataques básicos como: SYN FLOOD, ICMP FLOOD, UDP FLOOD, ETC; Detectar e bloquear a origem de PORTSCANS; Bloquear ataques efetuados por WORMS conhecidos; Possuir assinaturas específicas para a mitigação de ataques DOS E DDOS; assinaturas para bloqueio de ataques de buffer overflow; Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou ANTI-SPYWARE, permitindo a criação de exceções com granularidade nas configurações; Permitir o bloqueio de vírus e SPYWARES em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3; Identificar e bloquear comunicação com BOTNETS; Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de BOTNETS conhecidas; Os eventos devem identificar o país de onde partiu a ameaça; Deve incluir proteção contra vírus em conteúdo HTML e JAVASCRIPT, software espião (SPYWARE) e WORMS; Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos; Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, ETC, ou seja, cada

política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos; dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, SANDBOXING e verificação de call-back; A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

Filtro de URLs: Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); Deve ser possível a criação de políticas por grupos de usuários, IPS, redes ou zonas de segurança; Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active DIRECTORY e base de dados local; A identificação pela base do Active DIRECTORY deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall; Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo; Possuir pelo menos 60 categorias de URLs; Deve possuir a função de exclusão de URLs do bloqueio; Permitir a customização de página de bloqueio; Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados; Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário; Os requisitos de filtro de URL descritos acima aplicam-se apenas ao firewall das pontas remotas;

Identificação de usuários: Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active DIRECTORY, E-DIRECTORY e base de dados local; Deve possuir integração com Microsoft Active DIRECTORY para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários; Deve possuir integração e suporte a Microsoft Active DIRECTORY para o sistema operacional Windows Server 2012 R2 ou superior; Deve possuir integração com Microsoft Active DIRECTORY para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single SIGN-ON. Essa funcionalidade não deve possuir limites licenciados de usuários; Deve possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários; Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários; Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (CAPTIVE Portal); Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços; Deve suportar o envio e recebimento de credenciais via RADIUS;

Filtro de dados: Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, ETC) identificados sobre aplicações (HTTP, FTP, SMTP, ETC); Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos; Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos; Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

Geolocalização: Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados; deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

VPN CLIENT TO Site: Suportar IPSEC VPN; Suportar SSL VPN; Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies; Atribuição de DNS nos clientes remotos de VPN,

inclusive com DNS split TUNNEL; Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, ANTIPYWARE e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL; Suportar autenticação via AD/LDAP, certificado e base de usuários local; Suportar leitura e verificação de CRL (CERTIFICATE REVOCATION LIST); Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

Recursos Gerais de SD-WAN: A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação; Deve ser possível criar políticas que definam os seguintes critérios para match: Endereços de origem; Grupos de usuários; Endereços de destino; DSCP; Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e ETC); A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de HEALTH CHECK, permitindo testes de resposta por PING, HTTP, TCP/UDP ECHO, DNS, TCP-CONNECT E TWAMP; O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente, inclusive 4G; O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente; Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, JITTER, perda de pacote, banda ocupada ou todos ao mesmo tempo; A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub; Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio; A solução deve permitir a definição do roteamento para cada aplicação; Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação; Deve possibilitar a definição do link de saída para uma aplicação específica; Deve implementar balanceamento de link por HASH do IP de origem; Deve implementar balanceamento de link por HASH do IP de origem e destino; Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links; Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais; A solução de SD-WAN deve possuir suporte a POLICY BASED ROUTING ou POLICY BASED FORWARDING; Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões; Deve permitir a customização dos TIMERS para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido; A solução de SD-WAN deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP; Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como YOUTUBE, Facebook, ETC), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de SHAPING. Dentre as tratativas possíveis, a solução deve contemplar: Suportar a criação de políticas de QoS e TRAFFIC SHAPING por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta; O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio; O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo BEST-EFFORT/não corporativas, tais como Youtube, Facebook ETC; Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do BACKBONE para fins de reserva de banda; O QoS deve possibilitar a definição de fila de prioridade; Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPS de origem e destino, logins e portas; A capacidade de agendar intervalos de tempo em que as políticas de SHAPING/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço; Deve possibilitar a definição de bandas distintas para download e upload; A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do HEALTH CHECK (PACKET LOSS, JITTER e latência); A solução de SD-WAN deve suportar IPv6; Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN; Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo; O SD-WAN deverá possuir serviço de Firewall STATEFUL; A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN; A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site; Deve ser capaz de bloquear acesso às aplicações; Deve suportar NAT dinâmico bem como NAT de saída; Deve suportar balanceamento de tráfego por sessão e pacote; Suportar VPN

IPSEC SITE-TO-Site; A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (ADVANCED ENCRYPTION STANDARD); A VPN IPSEC deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512; A VPN IPSEC deve suportar DIFFIE-HELLMAN GROUP 1, GROUP 2, GROUP 5 e GROUP 14, GROUP 15 até 21 e GROUP 27 até 32; A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2); A VPN IPSEC deve suportar Autenticação via certificado IKE PKI; Deve suportar o uso de DDNS, para casos onde uma ou ambas as pontas possuam IPS dinâmicos; Deve suportar VPN dial UP, no caso da ponta remota não possui IP estático na WAN; Deve possuir suporte e estar licenciamento para uso de VRFS; A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance;

SOLUÇÃO DE CENTRALIZAÇÃO DE LOGS: A solução deve ser baseada em máquina virtual do mesmo fabricante da solução de NGFW e ter como objetivo a coleta, armazenamento e análise automatizada de registros em modo centralizado de todos os equipamentos a partir de uma única console de administração; Poderá ser entregue em formato de APPLIANCE virtual; Caso a solução ofertada seja em APPLIANCE virtual a contratante será responsável pelo fornecimento máquina virtual para instalação da licença. Deverá estar devidamente licenciada para: Suportar a coleta de, no mínimo, 25 GB de logs diários; Caso a solução seja entregue como APPLIANCE virtual, este deve suportar: Deve ser compatível com os HYPERVISOR VMWARE 6.5 e superiores, Hyper-V 2016 e superiores, e KVM; Não deverá existir limite para o número de VCPUS no APPLIANCE virtual; Não deverá existir limite para a expansão da memória RAM no APPLIANCE virtual; Deve suportar VMOTION com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve**;** Realizar o backup das configurações para permitir o retorno de uma configuração salva; Deve possuir licenciamento do fabricante com validade mínima de 60 (sessenta) meses; Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora; Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações; Deve suportar o conceito de MULTI-TENANCY visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução. A solução deve permitir o uso de APIs RESTFUL para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança; Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito; Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas; Utilizar técnicas de MACHINE LEARNING para a captura de índices de comprometimento, através de URLs, domínios e endereços IPS maliciosos; Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.; Deve oferece um portal do cliente fácil de usar, permitindo acesso às capacidades seguras de SD-WAN, como monitoramento e modelos SD-WAN, políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links; Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais; Suporte à geração de relatórios de tráfego em tempo real, em formato de mapa geográfico; Suporte à geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas; Suporte à geração de relatórios de tráfego em tempo real, em formato de tabela gráfica; Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado; Deve possuir mecanismos de remoção automática para logs antigos; Permitir importação e exportação de relatórios Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV; Deve permitir exportar os logs no formato CSV; Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário; Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor SYSLOG externo ou similar; A solução deve ter relatórios predefinidos; Deve permitir o envio automático dos logs para um servidor FTP externo a solução; Deve ter a capacidade de personalizar a capa dos relatórios obtidos; Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs; Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados; Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

Deve ter um mecanismo de "pesquisa detalhada" ou "DRILL-DOWN" para navegar pelos relatórios em tempo real; Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo; Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente; Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades; Permitir o envio por e-mail relatórios automaticamente; Deve permitir que o relatório seja enviado por e-mail para o destinatário específico; Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador; Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado; Deve permitir o uso de filtros nos relatórios; Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros; Permitir especificar o idioma dos relatórios criados; Gerar alertas automáticos via e-mail, SNMP e SYSLOG, com base em eventos especiais em logs, gravidade do evento, entre outros; Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo; Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios; Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros; Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado; Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos; Deve permitir visualizar em tempo real os logs recebidos; Deve permitir o encaminhamento de log no formato SYSLOG; Deve permitir o encaminhamento de log no formato CEF (Common EVENT Format); Deve suportar a configuração Master / SLAVE de alta disponibilidade em camada 3; Possuir a capacidade de receber logs de soluções de terceiros através de SYSLOG; A solução deverá disponibilizar EVENT HANDLERS nativos para geração, tratamento e enriquecimento de eventos de segurança a partir dos logs recebidos, permitindo o uso de regras básicas e regras de correlação, com parametrização por filtros, severidade, origem, destino, tipo de evento e demais atributos relevantes; A solução deverá possuir regras de correlação para detecção avançada de ameaças, permitindo identificar comportamentos suspeitos, encadeamento de eventos, anomalias operacionais e incidentes compostos, a partir da consolidação e correlação de logs de múltiplas fontes suportadas; A solução deverá disponibilizar PLAYBOOKS para automação de fluxos de resposta, investigação e tratamento de incidentes, permitindo criação, edição, execução e customização de PLAYBOOKS, inclusive por meio de templates pré-definidos e integração com conectores e ações automatizadas; Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados; Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de "Zero Day" encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição; Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo dela, tipos de indústria que já foram alvo do malware, comportamento malicioso conhecido sobre o malware e quais são os autores; Deve permitir gerar alertas de eventos a partir de logs recebidos; Deve suportar o serviço de Indicadores de Compromisso (IOC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça), o número de ameaças detectadas; A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato;

MEMÓRIA DE DIMENSIONAMENTO DOS REQUISITOS DE PERFORMANCE (NGFW)

Os requisitos mínimos de desempenho fixados para o NGFW não foram extraídos de catálogo de fabricante, mas calculados a partir da realidade da rede municipal, conforme abaixo:

a) **THROUGHPUT de firewall (26 GBPS):** o link de Internet contratado atualmente é de 1 GBPS, porém o tráfego interno Leste-Oeste entre VLANS e o tráfego de VPN SITE-TO-SITE somam, em pico medido, aproximadamente 8 GBPS. Aplica-se margem de crescimento de 100% para o horizonte de 60 meses (16 GBPS) e reserva de 60% para absorver o tráfego de FAILOVER do cluster ativo-passivo quando um dos appliances assume integralmente a carga (16 GBPS × 1,6 ≈ 26 GBPS). O valor de 26 GBPS é, portanto, o mínimo necessário para que o equipamento sobrevivente suporte sozinho a operação em caso de falha do nó principal, sem degradação dos serviços.

b) **THROUGHPUT de VPN IPSEC (35 GBPS):** decorre da necessidade de escoamento do tráfego criptografado SITE-TO-SITE e CLIENT-TO-SITE em cenário de FAILOVER, com margem de 35% sobre o valor de firewall, padrão de mercado para o perfil de tráfego do Município.

c) **Conexões simultâneas (11 milhões) e novas conexões por segundo (400 mil):** dimensionadas com base no número de sessões ativas por usuário (média de 250 sessões), no parque de 600 endpoints e na reserva para picos de abertura de sessões em horário de expediente, com margem de 30%.
d) **Atendimento por múltiplos fabricantes:** a pesquisa de mercado identificou pelo menos três fabricantes cujos modelos de 1U atendem, simultaneamente, a todos os requisitos acima, o que demonstra a ausência de direcionamento e a competitividade do certame (Súmula TCU nº 270).

SOLUÇÃO DE AUTENTICAÇÃO CENTRALIZADA E MFA: Deve ser fornecido para 100 usuários; Deve ser licenciado de forma a entregar todas as capacidades e funcionalidades descritas no termo de referência, com suporte e garantia por todo o período de contrato (60 meses) Deve incluir 40 tokens para aparelhos móveis para implementação de MFA, sendo que: Deve ser do tipo mobile e suportar autenticação em dois fatores através do aplicativo (iOS, Android); Deve oferecer proteção contra-ataques do tipo “BRUTE-FORCE”; Deve permitir a visualização do número de série no aplicativo; Deve suportar OATH e OTP. A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração, sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados; Deve suportar autenticação em dois fatores (TWO-FACTOR AUTHENTICATION);Deve possuir suporte a autenticação de dois fatores em pelo menos dois tipos diferentes de tokens, sendo o primeiro físico (token), e o segundo lógico como softwares para dispositivos móveis ou e-mail ou SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário. Licenciamento de SMS não inclusos nesta especificação; Deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais e ETC; Deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta; Deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade; Deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos; Deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação; Deve permitir a criação de novos usuários na base de dados local de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário; Deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que utilize o token como único fator de autenticação; Deve permitir associar os tokens aos usuários criados localmente na base de dados; Deve permitir que os próprios usuários façam o registro dos seus tokens e relatem a perda de um token automaticamente, sem necessidade de envolver um administrador; Deve permitir remoção automática em massa de usuários desabilitados, baseado em critérios definidos; Deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança; Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade; Deve prover um portal web para o auto registro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro, o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado; Deve funcionar como servidor RADIUS (Remote AUTHENTICATION Dial-In USER Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo; Deve suportar a integração com servidor RADIUS remoto; Deve ter capacidade de funcionar como servidor LDAP (LIGHTWEIGHT DIRECTORY Access PROTOCOL), proporcionando autenticação aos dispositivos compatíveis com tal protocolo; Deve suportar a integração com servidor LDAP remoto (como Microsoft Active DIRECTORY); Deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+; Deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone; Deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso; Deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes; Deve suportar Security ASSERTION Markup LANGUAGE (SAML), agindo como um Provedor de Identidade (INDENTITY PROVIDER - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de

Serviços (Service PROVIDER -SP); Deve permitir integração com bases do Azure DIRECTORY E GSUITE; Por meio do SAML, deve permitir integrações com SPS variados, tais como Office 365; Deve atuar como Autoridade Certificadora (CA); Deve permitir a administração de certificados digitais, com emissão e revogação; Deve permitir o uso de CA'S confiáveis para validação de certificados emitidos por CA'S externas; Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL); Deve prover repositório para autenticação de VPN SITE-TO-SITE através de Certificados; Deve suportar SCEP Server (SIMPLE CERTIFICATE ENROLLMENT PROTOCOL), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador; Deve ser capaz de importar outros certificados de CA'S assim como a lista de certificados revogados; Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários; Deve prover capacidade de serviço SSO (Single SIGN-ON), com autenticação transparente (passiva) de usuários em sistemas compatíveis; Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade se SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio; Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO; Deve suportar análise de arquivos SYSLOG enviados de fonte remota, para uso pelo serviço de SSO; Deve suportar Security ASSERTION Markup LANGUAGE (SAML), agindo como autenticador de um Provedor de Serviços (Service PROVIDER - SP) solicitando informações de identidade de usuários a Provedores de Identidade (INDENTITY PROVIDERS - IDP'S) de terceiros; Deve suportar SSO baseado em RADIUS (RSSO - RADIUS Single SIGN-ON); Deve suportar RSSO ACCOUNTING Proxy permitindo a recepção de pacotes RADIUS de ACCOUTING, a modificação destes pacotes e o encaminhamento dos mesmos para vários outros;

Solução de EPP e ZTNA: A solução de EPP e ZTNA deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas. Deve ser licenciado de forma a entregar todas as capacidades e funcionalidades descritas no termo de referência, com suporte e garantia por todo o período de contrato (60 meses) Por motivo de compatibilidade e interoperabilidade entre a solução de ZTNA e o Firewall, estes devem ser do mesmo fabricante. A solução de ZTNA deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em TAGS de Zero Trust. A solução de ZTNA deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão. Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem ou através do fornecimento de máquina virtual a ser provisionado no ambiente da CONTRATANTE. O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante. Deve ser compatível com pelo menos os seguintes sistemas operacionais: Windows, Linux e MacOS. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários. A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso. Deve ser possível revogar o certificado de um agente por meio da console central. O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso. No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados estejam diferentes, o acesso deverá ser bloqueado por padrão. Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional. Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug. Deve ser possível exportar os logs diretamente a nível de agente. Deve ser possível exigir uma senha para desconectar o agente da console central. Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente. Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central. Deve ser possível enviar os logs para uma ferramenta de

consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes. Deve ser possível ainda atribuir TAGS aos endpoints de acordo com o índice de comprometimento detectado pela solução de consolidação de logs, desde que haja licenciamento instalado para tal. Deve ser possível configurar o agente para usar Proxy. O agente deve permitir a configuração local via XML (EXTENSIBLE MARKUP LANGUAGE); deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central. Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML. Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente. Deve ser possível especificar a validade do código de registro. A console central de agentes deve dispor de métodos para determinar se um usuário está ON-NET ou OFF-NET, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários ON-NET e OFF-NET. A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4. Deve ser possível agrupar agentes em grupos. Deve ser possível atribuir grupos de agentes a perfis de políticas específicos. Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço MAC, IP público, estado da conexão com a console central, zero TRUST TAGS associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA. O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S. Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round ROBIN, por peso, baseado no host FIELD do cabeçalho HTTP ou baseado em disponibilidade do servidor. Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor. Deste modo, o agente deve manipular o host file do endpoint visando criar entradas DNS. Deve ser possível definir um pool de IPS no proxy de acesso como IPS de origem para comunicação interna com as aplicações privadas. A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas. As regras de conformidade devem gerar TAGS que são sincronizadas entre os elementos da solução de ZTNA visando controlar a postura de um determinado endpoint diretamente no proxy de acesso. A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de COMPLIANCE definidas. Deve ser possível construir TAGS com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVES, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas. A console central deve permitir exportar e importar tAGS entre sistemas diferentes por meio de um arquivo JSON. Deve ser possível verificar quais endpoints estão associadas com cada TAG. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma TAG simultaneamente, caso a política possua vínculo com diversas TAGS. Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, TAG ZTNA, grupo de usuários ou usuário. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, RADIUS ou base de dados local. Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de

segurança a nível de sistema operacional. Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente. Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos. Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de COMPLIANCE. Deve ser possível excluir determinadas aplicações da verificação de COMPLIANCE e até mesmo desabilitar o patch automático. O agente deve dispor de um sistema de notificação do tipo pop-up visando alertar o usuário. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente. Deve suportar a criação de várias versões de pacotes de instalação. As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDS, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente. Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (REGEX) com as opções de permitir, bloquear ou monitorar. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário. Deve ser possível determinar quando o filtro web entrará em ação no agente, e se deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa. Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, INLINE do inglês, visando controlar o acesso a aplicações SaaS. Deve suportar o envio de logs para um analisador central de logs, onde os índices de compromissos do cliente (IOC) seja processado (taxas de confirmação); suportar receber atualizações de assinaturas dinâmicas da solução de proteção avançada de ameaças (ATP) ou SANDBOXING;

FUNCIONALIDADE DE ANTI-MALWARE: O cliente de segurança deve ter a capacidade de inspecionar arquivos executáveis, bibliotecas e drivers quanto a vírus; O cliente de segurança deve ser capaz de verificar atualizações de assinatura automaticamente O cliente de segurança deve ser capaz de enviar arquivos para inspeção nos sistemas SANDBOXING do mesmo fabricante; O cliente de segurança deve ser capaz de bloquear os canais de comunicação usados por hackers ou atacantes; O cliente de segurança deve notificar localmente quando um vírus é detectado O cliente de segurança deve permitir que o usuário inicie uma verificação sob demanda O cliente de segurança deve permitir que a verificação de vírus seja iniciada automaticamente regularmente O cliente de segurança deve permitir a visualização dos arquivos em quarentena Deve permitir a configuração do perfil antivírus a partir do console central do mesmo fabricante Deve ter uma solução de proteção contra malware baseada em nuvem. Essa proteção deve ser capaz de gerar uma soma de verificação do arquivo acessado e consultar a nuvem se essa soma de verificação corresponder a uma nova ameaça. A ferramenta de proteção baseada em nuvem NÃO deve enviar o arquivo inteiro ou seus metadados. SOMENTE a soma de verificação A ferramenta de proteção baseada em nuvem deve analisar apenas arquivos de alto risco, como, entre outros, documentos do Word, Excel, PDF e DLL. Deve ter uma solução de Anti-Exploit, que protege o endpoint de ameaças em tempo real, observando o comportamento de aplicativos populares, incluindo os leitores do Office, Internet Explorer, Chrome, Firefox, Java, Java, Flash e PDF ETC; Deve ser capaz de proteger arquivos, tipos de arquivos específicos ou pastas contra alterações não autorizadas; Caso seja detectando um comportamento de criptografia não autorizada (Ransomware) do arquivo ou pasta, à solução deve ser capaz de restaurar o arquivo; Deve ser capaz de enviar arquivos para uma solução de proteção avançada de ameaças (ATP) (ou SANDBOXING) antes de ser acessado; Deve suportar sando localmente ou através de uma solução em nuvem; Deve ser capaz de bloquear o acesso ao arquivo

até que o SANDBOX dê um veredicto; Caso um arquivo seja marcado como malicioso pela SANDBOX, o mesmo deve ser mantido em quarentena.

SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO: Deve permitir o gerenciamento centralizado de acessos privilegiados; Deve ser licenciado de forma a entregar todas as capacidades e funcionalidades descritas no termo de referência, com suporte e garantia por todo o período de contrato (60 meses) Deve estar dimensionado e licenciado para até cinquenta (45) agentes; Entende-se por acessos privilegiados os tipos de acesso a ativos e a sistemas de tecnologia, além dos acessos realizados por um usuário comum, geralmente realizados por administradores de redes, administradores de servidores e administradores de sistemas; A solução deve controlar o acesso baseado em função, com recursos de auditoria e de segurança, provendo no mínimo as seguintes funcionalidades: Cofre de credenciais: funcionalidade onde os usuários não precisam ter conhecimento das credenciais, reduzindo-se o risco de vazamento, incluindo o rotacionamento automático dessas credenciais; Controle de acesso a contas privilegiadas: funcionalidade onde é possível estabelecer níveis de privilégios de cada usuário, incluindo funcionalidades de fluxo de aprovação de acessos a determinados recursos; Monitoramento e registro de eventos: funcionalidade onde é possível monitorar, registrar e auditar as atividades dos usuários privilegiados, incluindo informações das sessões tais como pressionamento de teclas, eventos de mouse, etc.; solução deve ser do tipo APPLIANCE virtual, compatível com pelo menos os HYPERVISORS VMWARE ESXI, MICROSOFT HYPER-V E LINUX KVM, sendo de responsabilidade da contratante a disponibilização dos recursos necessários para a implantação da solução: hardware e software (HYPERVISOR); A solução deve suportar a implementação em cluster de alta disponibilidade (HA), com suporte a implementação de um nó remoto para fins de Disaster Recovery; As chaves criptográficas devem ser armazenadas internamente na solução e protegidas por tecnologia TPM ou VTPM; A solução deve ter a possibilidade de integração com o item “SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO” e com o item “SOLUÇÃO DE ZTNA” deste processo, sendo possível, portanto, o uso da autenticação centralizada e de TAGS Zero-Trust; A solução deve prover interface de API para integração com sistemas ou soluções de terceiros; A solução deve diferenciar os usuários da plataforma entre: Usuários comuns: aqueles que apenas executam as tarefas de gerenciamento dos sistemas de destino, como por exemplo a equipe de TI, um contratado da TI, um administrador de banco de dados (DBA). Geralmente estes usuários são Gerentes de TI e Administradores de Sistemas de TI. Usuários administradores: aqueles que são responsáveis pelas tarefas de gerenciamento da solução. A solução deve operar pelo menos nos seguintes modos: Modo Proxy: toda conexão aos sistemas de destino é interceptada pela solução, que fica responsável pela conexão final ao sistema de destino. Nesse modo, a máquina cliente não tem acesso direto as credenciais de acesso e o administrador da solução pode interromper conexões se um comportamento estranho for detectado; Modo Não-Proxy: toda conexão aos sistemas de destino parte diretamente da máquina cliente e a solução fornece ao cliente as credenciais para esse acesso; A solução deve armazenar de forma segura o nome de usuário e a senha/chave dos servidores como segredos. Os segredos podem conter informações sobre login, credenciais e o endereço IP do servidor de destino. O usuário final pode usar o segredo para acessar os servidores; as credenciais reais devem ser protegidas e os usuários da solução não podem acessar as credenciais, exceto em alguns casos configuráveis pelo administrador. As credenciais de login podem ser alteradas automaticamente e também manualmente, a depender dos diferentes casos de uso; A solução deve permitir a configuração de políticas comuns e um sistema de fluxo de aprovação hierárquico e editável para acesso a informações sensíveis; Os critérios de gerenciamento de senha devem ser configuráveis para atender à política organizacional de frequência de alteração de senha/controle de aprovação de uso/alteração após o uso; Deve incluir e não se limitar os seguintes recursos de Sistemas e Protocolos e Ferramentas: AD, Windows, Linux/Unix, Oracle DB, MS SQL, CISCO, AS400, Microsoft SQL, Microsoft SQL Shell, MySQL CLI, MySQL Shell, PostgreSQL CLI, VNC, WEB SMB, WEB SSH, Web RDP, Web SFTP; Deve permitir a construção de um conector de plataforma personalizado e integração A2A; Deve oferecer suporte para aprovação de credencial dupla, exigindo aprovações de usuários designados antes de permitir o acesso a credenciais para contas gerenciadas; Deve oferecer suporte a funcionalidades de fluxo de trabalho para controles de liberação de senha e sessão, incluindo suporte para vários níveis de autorização, capacidade de agrupar autorizadores; Deve suportar a capacidade de expirar a solicitação de aprovação após um período de tempo; Deve fornecer a capacidade de permitir recursos de checkout e check-in para SECRETS; Deve permitir a autenticação de uma sessão sem revelar a senha por meio da máquina

do usuário final; Sessões privilegiadas devem ser transmitidas por proxy por meio de um hardware seguro ou dispositivo virtual; O proxy de sessão deve ser capaz de entrar em uma conta sem liberar uma senha para o usuário privilegiado; A solução deve permitir o uso do modo cliente, com o uso de agentes, e deve oferecer suporte ao modo somente navegador, onde nenhum software cliente/agente é necessário; Os seguintes modos de cliente e navegador devem ser suportados: Modo cliente: PUTTY, Windows Remote Desktop, REALVNC, TIGHTVNC e WINSCP etc.; Modo de navegador: Web SSH, Web RDP, Web VNC, Web SMB, Web SFTP e Web ACCOUNT; No modo navegador, deve possibilitar o uso de pelo menos as seguintes funcionalidades: acesso a senhas, sessões e administração da solução; Deve possuir iniciadores de conexão para pelo menos: MySQL (CLI e Shell), Microsoft SQL CLI, PostgreSQL CLI, SSH (PUTTY, SSH CLI e SECURECRT), Remote Desktop e VNC (TIGHTVNC e VNC VIEWER); As sessões devem permitir a inclusão ou exclusão de comandos executados durante uma sessão sem a necessidade de um agente; Deve suportar registro/monitoramento de pelo menos os seguintes protocolos de sessão - Telnet, SSH, RDP, ICA, VNC, SQL Plus, SQL Windows, Http & Https, x5250, x3270; Deve permitir a auditoria das atividades administrativas da própria solução; As solicitações de acesso privilegiado devem ser feitas usando um modelo de solicitação/liberação, no mínimo; Não deve permitir que um administrador da solução realize o BYPASS do fluxo de aprovação para obter uma senha ou ativar uma sessão; A solução deve oferecer suporte à sessão remota de auditoria no modo não transparente ou transparente, sem alteração no fluxo de trabalho para acessar a sessão remota usando ferramentas nativas do cliente, incluindo injeção direta de credencial; Deve suportar monitoramento e gravação de sessão (para análise posterior) e seu monitoramento em tempo real (para vigilância em tempo real), permitindo que o administrador encerre as sessões, caso necessário; As gravações do vídeo da sessão devem usar formatos disponíveis publicamente; Deve ser possível gerar alertas de e-mail quando um usuário executa um comando restrito e a detecção de tais comandos não devem depender do uso de agentes; Deve suportar diferentes métodos de autenticação e integração com sistemas corporativos como: Active DIRECTORY, LDAP, SAML, RADIUS; Deve possuir suporte a múltiplo fator de autenticação (MFA) através de Token da Solução, SMS e E-Mail; Deve permitir a configuração de OTP (ONE Time PASSWORD) via e-mail; Deve permitir a verificação de arquivos transferidos entre o endpoint e os ativos protegidos, realizando-se a varredura contra conteúdos maliciosos; Deve suportar o uso de verificações contra vazamento de dados (DLP) nos arquivos transferidos; Deve suportar o bloqueio da área de transferência dos ativos privilegiados, para impedir a cópia de informações desses ativos; Deve fornecer a funcionalidade de Break Glass para acesso emergencial as credenciais armazenadas na solução; Deve restringir o acesso a console dos ativos protegidos pela solução; Deve proteger o acesso à rede dos ativos protegidos pela solução; Deve armazenar todas as senhas em um cofre seguro com criptografia AES-256; Deve permitir que qualquer login/senha usados para acesso a ativos protegidos seja armazenado internamente e com segurança e deve permitir que os usuários se conectem aos ativos protegidos sem o conhecimento do login/senha utilizado; Deve alterar automaticamente as senhas para um grupo de recursos; Deve estabelecer acesso granular às senhas; Deve impedir os usuários vejam a senha em texto puro; Deve permitir que as credenciais sejam injetadas diretamente nos sistemas, dando acesso aos usuários sem que eles vejam ou forneçam credenciais; Deve suportar o controle de acesso sem o uso de VPN; Deve permitir que as sessões sejam mantidas e compartilhadas com os auditores para interação (colaboração de sessão); Deve permitir que os auditores monitorem usuários privilegiados sob demanda e em tempo real; Deve integrar um sistema de fluxo de trabalho para permitir o acesso administrativo às máquinas identificadas; A solução deve permitir acesso ao recurso de destino, sem agente, pelo menos nos protocolos RDP, SSH, TELNET, VNC, HTTPS; Deve possibilitar o bloqueio do usuário no caso de uma execução de uma ação restrita; Deve permitir rastreabilidade das conexões; Deve permitir visualizar todas as conexões ativas; Deve permitir rastreabilidade e controle de transferências de arquivos; Deve permitir a configuração de notificações de e-mail em um determinado número de indicadores, como eventos relacionados ao tráfego (falha de conexão, falha de autenticação, etc.); Deve permitir integração com soluções SIEM para relatórios avançados e processamento em tempo real de detecção de comportamento malicioso; Deve possuir logs de auditoria completos e pesquisas avançadas, como pesquisas de texto para isolar incidentes; Os logs de auditoria da solução devem mostrar claramente quem acessou qual dispositivo de destino, bem como a duração (hora de início e hora de término); Deve fornecer logs para o histórico de aprovação de sessões privilegiadas; Deve possuir um painel para exibir os usuários conectados no momento; Deve permitir relatórios personalizáveis.

1.2 Valor máximo estimado da contratação: R$ 2.635.894,80 (dois milhões, seiscentos e trinta e cinco mil, oitocentos e noventa e quatro reais e oitenta centavos).

1.3.Da natureza do objeto
(X) Não se enquadra como sendo bem de luxo, conforme Decreto Federal n.º 10818/2021
(X) Os bens objeto desta contratação são caracterizados como comuns, com características e especificações usuais de mercado.

2. JUSTIFICATIVA DA CONTRATAÇÃO
2.1. Justificativa Técnica da Solução Integrada e do Agrupamento
Conforme demonstrado no Estudo Técnico Preliminar (ETP) e no Documento de Formalização da Demanda (DFD), a solução foi concebida como uma plataforma integrada de segurança cibernética e gestão segura de identidade, cujos componentes apresentam elevado grau de integração e interdependência funcional.
O agrupamento do objeto em lote único representa a alternativa tecnicamente mais adequada e economicamente mais vantajosa para a Administração Municipal, afastando-se o parcelamento do objeto em itens isolados pelas seguintes justificativas técnicas:

- Os mecanismos de proteção perimetral, gerenciamento centralizado, gestão de logs, proteção de *endpoints*, gerenciamento de identidades e acessos (IAM), gerenciamento de acessos privilegiados (PAM), autenticação multifator (MFA) e acesso seguro baseado em *Zero Trust* (ZTNA) devem operar de forma integrada, compartilhando informações, eventos e políticas de segurança. Essa integração permite maior eficiência na prevenção, identificação e mitigação de ameaças, além de proporcionar administração centralizada de toda a infraestrutura de segurança da informação.
- A contratação em lote único assegura que um único fornecedor seja responsável pelo fornecimento, implantação, integração, suporte técnico, atualizações e garantia da solução, reduzindo riscos de incompatibilidade entre plataformas, conflitos de responsabilidade ("jogo de empurra" técnico) e dificuldades na identificação e correção de falhas. Essa abordagem contribui para maior eficiência operacional, simplificação da gestão contratual e adequada continuidade dos serviços de Tecnologia da Informação.

2.2. Justificativa do Modo de Disputa
Para a condução da etapa competitiva do Pregão Eletrônico, adota-se o modo de disputa aberto e fechado, visando ampliar a competitividade entre os licitantes, incentivar a apresentação de propostas mais vantajosas e assegurar a seleção da proposta mais benéfica para a Administração. Considerando a complexidade da solução, sua elevada integração tecnológica e o valor estimado da contratação, o procedimento foi estruturado para proporcionar ampla participação do mercado, garantindo condições adequadas para obtenção da melhor relação entre qualidade técnica, desempenho e custo durante todo o ciclo de vida da solução.

2.3. Alinhamento com os Requisitos de SLA e Atendimento Continuado
Considerando a natureza da solução contratada, justifica-se a definição de Acordos de Nível de Serviço (SLA) para assegurar a disponibilidade dos equipamentos, softwares, licenças, subscrições e serviços especializados durante toda a vigência contratual. Os níveis mínimos de atendimento estabelecem prazos rígidos para diagnóstico e resolução de falhas (como a contenção de incidentes de severidade altíssima em até 4 horas), observando a criticidade das ocorrências e garantindo a continuidade da infraestrutura tecnológica da Administração Municipal.

2.4. Justificativa da Vigência de 60 Meses
O prazo de vigência da contratação será de 60 (sessenta) meses, fundamentado nas seguintes premissas operacionais e legais:

- O monitoramento pelo Centro de Operações de Segurança (SOC) operando em regime 24x7x365 e as subscrições dinâmicas de segurança configuram-se como serviços e fornecimentos contínuos, uma vez que a interrupção dessa blindagem digital paralisaria as atividades críticas do município (saúde, arrecadação, segurança). A legislação vigente permite de forma direta o estabelecimento de contratos iniciais de até 5 anos para estes cenários.

- A fixação do prazo inicial em 60 meses garante a diluição e a amortização dos custos iniciais de engenharia (instalação física, migração complexa de regras de rede e treinamento da equipe de TIC). Além disso, o prazo estendido blinda o erário municipal contra oscilações cambiais agressivas no mercado de tecnologia e assegura previsibilidade e estabilidade de preços a longo prazo.

3. DOS PARÂMETROS DA LICITAÇÃO
3.1 Defina e justifique a modalidade de licitação/ contratação direta:
(X) pregão
A modalidade de licitação definida é o Pregão (na forma eletrônica), pois os bens e serviços objeto desta contratação são caracterizados como comuns, possuindo características e especificações usuais de mercado. Nos termos da Lei Federal nº 14.133/2021, o pregão é a modalidade obrigatória para a aquisição de bens e serviços comuns, cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, garantindo ampla competitividade e a seleção da proposta mais vantajosa para a Administração Pública.

3.2.Será adotado o Sistema de Registro de Preços – SRP?
(X) Não

3.2.1 Foram verificadas intenções de registro de preços e atas de registro de preços de outros órgãos?
(X) não
Justificativa para a não realização de adesão:
A não realização de adesão a Atas de Registro de Preços (ARP) de outros órgãos justifica-se pela alta especificidade, customização e complexidade da solução integrada de segurança cibernética demandada pelo Município de Quatro Barras. O objeto não se limita ao simples fornecimento de equipamentos de prateleira, mas engloba a prestação de serviços continuados por 60 meses, incluindo monitoramento ininterrupto por Centro de Operações de Segurança (SOC 24x7x365), implantação física no Datacenter local, e a migração complexa de regras de rede e integração com sistemas legados (como a telefonia VoIP do município).
Atas de outros órgãos possuem dimensionamentos, quantitativos exatos de licenças (como os 600 *endpoints*, 100 usuários MFA e 45 agentes PAM específicos de Quatro Barras) e Acordos de Nível de Serviço (SLAs) modelados exclusivamente para as suas próprias realidades topológicas e operacionais. Dessa forma, o aproveitamento de um registro de preços de terceiros inviabilizaria o atendimento integral dos níveis de segurança e das exigências de suporte técnico local previstos neste planejamento.

3.3.Será adotado tratamento diferenciado a microempresas (ME) e empresas de pequeno porte (EPP), conforme o disposto no art. 48 da Lei Complementar nº 123/2006 (alterado pela Lei Complementar nº 147/2014):
(X) Valor referencial superior a R$ 80.000,00 – não se aplica por tratar-se de serviço.

3.4.Haverá necessidade de vistoria prévia (visita técnica)?
(X) Não será exigida vistoria.
Justificativa:
A não exigência de vistoria prévia fundamenta-se no art. 63, § 2º, da Lei Federal nº 14.133/2021 e na jurisprudência pacificada do TCE/PR. Os requisitos técnicos, a volumetria da rede e as metas de SLA do SOC 24x7x365 foram descritos de forma clara, exaustiva e suficiente no Termo de Referência, permitindo a perfeita elaboração das propostas sem a necessidade de visita presencial.
A dispensa dessa obrigatoriedade evita custos desnecessários e barreiras geográficas, atraindo grandes integradores nacionais de Tecnologia da Informação e garantindo maior disputa e economicidade ao certame. Em conformidade com o art. 63, § 3º da lei regente, a vistoria é substituída pela exigência de uma Declaração de Pleno Conhecimento das Condições da Contratação, na qual a licitante assume total responsabilidade pelo dimensionamento e execução correta do ecossistema de segurança.

3.5.Será admitida a participação de consórcios?
(X) Não

Se assinalou não, justifique:
A vedação a consórcios justifica-se pela ampla competitividade no mercado de integradores de TI, que são plenamente capazes de fornecer individualmente todo o ecossistema exigido. Sendo uma contratação crítica de segurança cibernética com vigência de 60 meses, a formação de consórcios geraria riscos operacionais e pulverização de responsabilidades no cumprimento das metas rigorosas do SOC (24x7x365). A medida garante uma responsabilidade técnica única e estável, alinhada ao art. 15 da Lei nº 14.133/2021 e à jurisprudência do TCE/PR.

3.6.Será admitida a participação de cooperativas?
(X) Não
Se assinalou não, justifique:
A vedação à participação de sociedades cooperativas fundamenta-se no art. 16 da Lei Federal nº 14.133/2021. O objeto licitado exige a prestação de serviços continuados de monitoramento por Centro de Operações de Segurança (SOC 24x7x365), o que demanda subordinação jurídica imediata e o cumprimento de metas rigorosas de Acordos de Nível de Serviço (SLA), como a contenção de incidentes em até 4 horas.
A natureza do trabalho associado e autônomo das cooperativas fragilizaria a fiscalização do contrato plurianual e a garantia de continuidade da segurança lógica dos dados do Município. Além disso, a comercialização de ativos e licenças proprietárias globais de cybersecurity é feita por integradores comerciais tradicionais, desconfigurando a atividade-fim do cooperativismo. Essa restrição está em estrita consonância com a jurisprudência do Tribunal de Contas do Estado do Paraná (TCE/PR) para licitações complexas de Tecnologia da Informação.

3.7.Será admitida a subcontratação?
(X) Não

3.8. Do agrupamento de itens em lotes
A aquisição/contratação se dará em lotes?
(X) Não
Justificativa:
A opção pelo não parcelamento e agrupamento em Lote Único (Adjudicação por Preço Global) fundamentam-se no art. 47, II, da Lei Federal nº 14.133/2021 e na jurisprudência do TCE/PR. A medida assegura a inseparabilidade funcional do ecossistema de segurança cibernética (permitindo automação cruzada imediata entre firewalls e endpoints em caso de ataques), fixa a responsabilidade técnica e contratual sobre um único fornecedor e gera ganhos de economia de escala durante os 60 meses de vigência.

3.9 Defina e justifique o critério de julgamento:
(X) menor preço

Justificativa:
A adoção do critério de julgamento por Menor Preço (aplicado ao valor global do Lote Único) justifica-se por se tratar da contratação de bens e serviços comuns de Tecnologia da Informação. As especificações técnicas, exigências de desempenho dos firewalls, volumetria de licenças e as metas rígidas de Acordos de Nível de Serviço (SLA) para o monitoramento 24x7x365 foram descritas de forma clara, objetiva e exaustiva no Termo de Referência. Deste modo, uma vez assegurado o atendimento integral a todos os requisitos técnicos mínimos e às exigências de qualificação por parte dos licitantes, o critério do Menor Preço é o que melhor atende aos princípios da Economicidade, da Eficiência e do interesse público, garantindo a seleção da proposta mais vantajosa para a Administração Pública.

3.10 Defina o modo de Disputa:
(X) aberto/fechado
Justifique:
A escolha do modo de disputa aberto e fechado fundamenta-se na busca pela ampliação da competitividade e pela obtenção da proposta mais vantajosa para a Administração Pública, em estrita observância ao art. 56 da Lei Federal nº 14.133/2021.

Por se tratar de uma contratação de grande porte e alta complexidade tecnológica (Lote Único com fornecimento de ativos, licenças de software e prestação de serviços continuados de monitoramento por SOC 24x7x365), a combinação das etapas aberta e fechada permite, incialmente, a apresentação de lances públicos e sucessivos para o balizamento de preços. Em seguida, a etapa fechada estimula os licitantes melhor classificados a ofertarem suas melhores propostas de valor global sigilosamente, prevenindo estratégias meramente protelatórias de cobrir ofertas por centavos e garantindo o máximo desconto para o erário municipal.

3.11 Haverá inversão de fases:
(X) não

4. DOS CRITÉRIOS DE ACEITAÇÃO DA PROPOSTA
4.1.Serão exigidos documentos adicionais juntamente com a proposta de preços
(X) Sim
Se sim, quais?
Para fins de julgamento e classificação da proposta de preços, para estrita análise da equipe técnica da TIC, a licitante classificada em primeiro lugar deverá apresentar, no prazo fixado no edital, os seguintes documentos complementares:

1. **Catálogos Técnicos e Folhas de Dados (Datasheets):** Documentação técnica oficial do fabricante, emitida em língua portuguesa ou acompanhada de tradução, acompanhada de uma Matriz de Aderência (Modelo I), que comprove de forma clara e objetiva o atendimento individual a todos os requisitos de desempenho físico e lógico fixados no Termo de Referência.

MODELOS DE APRESENTAÇÃO PARA VERIFICAÇÃO TÉCNICA
MODELO I: DECLARAÇÃO DE ADERÊNCIA TÉCNICA (MATRIZ DE COMPATIBILIDADE)
(A ser apresentada em papel timbrado da empresa licitante, preenchida pela engenharia técnica)
À
Pregoeira do Município de Quatro Barras/PR
Ref.: Matriz de Aderência Técnica - Pregão Eletrônico nº XX/2026
Apresentamos a correlação objetiva entre os requisitos mínimos descritos no Termo de Referência e as especificações dos produtos/serviços efetivamente ofertados em nossa proposta:

Item	Requisito / Descrição Resumida do Item	Qtd / Und	Fabricante / Modelo Ofertado	Página do Catálogo / Datasheet Anexo	Critério de Atendimento
1	Firewall para Segurança de Rede: Fornecimento de Appliance (hardware + software) em modo cluster (alta disponibilidade ativo-passivo), com THROUGHPUT mínimo de 26 GBPS (Firewall) e 35 GBPS (VPN). Formato rack (máx. 1U). Deve incluir suporte a SD-WAN, filtro de conteúdo, IPS, antivírus de gateway, AntiSpam e licenciamento de subscrições para o período contratual.	2 UN	[Preencher]	Pág. XX	( ) Atende Integralmente ( ) Não Atende
2	Armazenamento de Logs: Fornecimento em máquina virtual. Centralização de logs e geração de relatórios com coleta mínima de 25GB de logs diários e licenciamento de subscrições para o período contratual.	1 UN	[Preencher]	Pág. XX	( ) Atende Integralmente ( ) Não Atende
3	Proteção Avançada para Estações: Composta com EPP e ZTNA, com suporte para no mínimo os seguintes sistemas operacionais: Windows,	600 LIC	[Preencher]	Pág. XX	( ) Atende Integralmente

	Linux e MacOS. Licenciamento de subscrições para o período contratual.				( ) Não Atende
4	Proteção Avançada para Gestão Segura de Identidade: AUTHENTICATOR com 100 Licenças de uso de software de autenticação multifator (MFA), em conformidade com a LGPD, com suporte a 10 soft tokens móveis (PUSH, QR CODE, OTP), portal Single SIGN-ON (SSO), sincronismo nativo com AD/LDAP. Licenciamento de subscrições para o período contratual.	1 UN	[Preencher]	Pág. XX	( ) Atende Integralmente ( ) Não Atende
5	Solução de Acesso Privilegiado (PAM): Software de segurança para gerenciamento, controle e monitoramento das contas com acesso privilegiado aos servidores de missão crítica. Licenciamento de subscrições para o período contratual.	5 SERV	[Preencher]	Pág. XX	( ) Atende Integralmente ( ) Não Atende
6	Treinamento: Serviço de capacitação técnica para até 10 profissionais indicados (e até 3 ouvintes), com carga horária mínima de 24 horas, incluindo fornecimento de material didático oficial e emissão de certificados oficiais. Deverá ser fornecido 4 vouchers para certificação oficial do fabricante (nível inicial).	5 SERV	[Preencher]	Pág. XX	( ) Atende Integralmente ( ) Não Atende
7	Implantação: Serviço de instalação física, cabeamento, configuração, ativação e migração integral de regras/políticas vigentes na rede municipal. O prazo de execução é de até 30 dias, com posterior entrega de documentação "As BUILT" editável.	9 SERV	[Preencher]	Pág. XX	( ) Atende Integralmente ( ) Não Atende

Local e Data
Nome, Assinatura Eletrônica e CPF do Responsável Técnico/Engenheiro

4.2. Será exigida amostra do(s) produto(s)/demonstração do(s) serviço(s):
(X) Não

4.3.Será exigida prova de conceito?
(X) Sim
Se sim:
Prazo para apresentação/demonstração: A licitante classificada provisoriamente em primeiro lugar será convocada pela Pregoeira e disporá de **até 30 (trinta) dias corridos**, contados da convocação, para a **instalação e configuração** do ambiente de testes. Concluída a instalação, os testes serão executados em **até 10 (dez) dias úteis consecutivos**, em sessões diárias, culminando na emissão de Parecer Técnico Final de Conformidade. O prazo total entre a convocação e a conclusão dos testes é de, no máximo, **40 (quarenta) dias corridos**. A licitante poderá, às suas expensas, antecipar a instalação para reduzir o prazo total. Caso a instalação ocorra em prazo inferior a 30 dias, os 10 dias úteis de teste serão contados a partir da comunicação formal de conclusão da instalação à fiscalização.
Da razoabilidade do prazo: O prazo de 10 (dez) dias úteis para execução dos testes foi definido em observância ao princípio da razoabilidade e à jurisprudência do TCE/PR (v.g. DETCPR 3700 –

Representação), que veda prazos exíguos que inviabilizem a participação de licitantes tecnicamente aptas. O prazo é suficiente para a realização da bateria completa de testes de desempenho e carga, das verificações funcionais e da auditoria de logs, sem prejuízo da competitividade. Ademais, a previsão de instalação prévia e a fixação de prazo total de até 40 dias corridos asseguram que a etapa não constitua barreira à participação de empresas de grande porte, em conformidade com o Prejulgado nº 22 do TCE/PR.

Endereço de entrega/demonstração: As atividades do teste de conformidade poderão ser executadas nas dependências do Prédio da Prefeitura: Av. Dom Pedro II, nº 110 – Centro, Quatro Barras – PR, CEP 83.420-001, ou realizadas de forma remota, a exclusivo critério da **CONTRATANTE.**

- **Critérios de avaliação (Critério de avaliação das amostras/protótipos):**

1. **Acompanhamento, Equipe e Responsabilidade:**

A convocada deverá indicar sua equipe técnica (composta por até 5 técnicos/representantes do licitante, do fabricante ou de empresa especializada em testes de bancada) responsável pela demonstração.

O teste será obrigatoriamente executado por técnico especialista capacitado pelo fabricante.

Todos os custos, equipamentos geradores de tráfego, simuladores de incidentes e ferramentas para execução do teste correm exclusivamente por conta da licitante convocada, sem ônus ao Município.

É permitido às demais licitantes homologadas acompanhar presencial/remotamente a sessão de testes para aferir a conformidade com o caderno de provas.

A licitante deverá enviar à CONTRATANTE a Tabela de Características e Valores (Requisito – Descrição – Valor Esperado – Atendimento S/N) com antecedência mínima de 1 (uma) semana da data marcada para a realização dos testes.

2. **Bateria de Testes Mínimos de Desempenho e Carga (Executados em Regime Contínuo por 30 Minutos):**

Teste em protocolo UDP com pacotes de 64 bytes (pior cenário), exigindo taxa sustentada mínima de 26 GBPS por no mínimo 30 minutos.

Teste em protocolo HTTP com pacotes de 1 byte, exigindo a manutenção sustentada de no mínimo 10.000.000 (dez milhões) de conexões TCP simultâneas por 30 minutos.

Teste em protocolo HTTP com pacotes de 1 byte, exigindo a taxa mínima de 390.000 (trezentas e noventa mil) novas conexões TCP por segundo durante 30 minutos.

Com ativação simultânea de Firewall, IPS, Controle de Aplicações, ANTI-BOT, Filtro de URL, Anti-MALWARE, Inspeção SSL e geração de Logs. Tráfego 100% em HTTPS (TLS 1.2, cifra ECDHE-ECDSA-AES128-GCM-SHA256, chave de 256 bits, pacotes de 128k), exigindo desempenho mínimo sustentado de 6,5 GBPS por no mínimo 30 minutos.

3. **Regras Operacionais e Condições durante os Testes:**

É vedado habilitar mecanismos de conservação de recursos, *BYPASS* automático de tráfego ou pacotes Jumbo Frame.

Todas as assinaturas de IPS e Malware devem permanecer habilitadas em modo de detecção.

É vedado o reinício do equipamento/sistema operacional entre as fases do teste e não é permitida a alteração dos tamanhos de pacotes estipulados.

As conexões TCP devem ser obrigatoriamente finalizadas com a flag FIN (sendo vedado o encerramento prematuro por RST).

A console de gerência deve permanecer acessível para auditoria, consulta de logs e alteração de políticas durante toda a aplicação de carga.

É permitida a instalação e a configuração prévia do ambiente de testes pela licitante convocada, às suas expensas, antes do início da contagem dos 10 (dez) dias úteis de execução, desde que comunicada formalmente à fiscalização e que a configuração seja validada no primeiro dia de testes.

A instalação prévia não dispensa a licitante da comprovação de todos os requisitos funcionais e de desempenho durante a bateria de testes.

4. **Critérios Objetivos de Reprovação/Desclassificação:**

Incapacidade de manter o THROUGHPUT mínimo exigido (admitindo-se variação limite de até 2% para valor menor). Apresentação de perda de pacotes absoluta superior a 1%.

Taxa de erros absolutos irrecuperáveis nas transações TCP/Camada 7 superiores a 0,5%.

Incompatibilidade técnica, omissão ou não comprovação integral de qualquer funcionalidade solicitada no Termo de Referência ou no Caderno de Provas.
A reprovação em qualquer item da PoC enseja a desclassificação total da proposta comercial, convocando-se a segunda colocada.

4.4. Será exigida carta de solidariedade do fabricante?
(X) Não

4.5. Será exigida garantia de proposta?
(X) Não

5. DOS CRITÉRIOS DE HABILITAÇÃO
Conforme o item 12 do edital.

6.DA EXECUÇÃO DO OBJETO
6.1.Prazo de entrega/execução
A execução das etapas do objeto dar-se-á nos seguintes prazos, contados a partir do dia útil seguinte ao recebimento da Nota de Empenho, Ordem de Serviço ou documento equivalente:

- Até 30 (trinta) dias úteis para a entrega física de todos os ativos de hardware no Datacenter, montagem em rack, cabeamento, migração completa da matriz de regras de rede, ativação em massa das subscrições lógicas (EPP, ZTNA, MFA e PAM) e homologação do ambiente com a entrega do relatório técnico As BUILT.
- Até 45 (quarenta e cinco) dias úteis para a conclusão e entrega do Serviço de Transferência de Conhecimento (Treinamento Técnico Oficial com carga horária mínima de 24 horas e fornecimento dos vouchers de certificação) para a equipe da Diretoria de TIC.
- 60 (sessenta) meses consecutivos para a prestação dos serviços continuados de suporte técnico, atualizações dinâmicas de segurança e monitoramento proativo via Centro de Operações de Segurança (SOC 24x7x365), contados a partir da assinatura do Termo de Recebimento Definitivo da implantação inicial.

6.2. Local, horário e endereço de entrega
Local de Entrega e Ativação Lógica:
Endereço Completo: Prefeitura Municipal de Quatro Barras, Av. Dom Pedro II, nº 110 – Centro – Quatro Barras – PR, CEP 83.420-000.
Horário de Recebimento: Os bens físicos e as equipes técnicas da CONTRATADA para a instalação presencial serão recebidos exclusivamente em dias úteis, de segunda a sexta-feira, das 08h00 às 12h00 e das 13h30 às 16h30, mediante prévio agendamento com a fiscalização do contrato.
Nota Operacional: A janela de virada de chave e homologação final dos Firewalls poderá ocorrer fora do expediente tradicional (finais de semana ou madrugadas) para evitar a paralisação dos serviços públicos essenciais (saúde, arrecadação, segurança), desde que previamente acordada e autorizada pelo Departamento de TI.

6.3. Bens perecíveis
(X) Não

6.4. Garantia de execução do contrato
Será exigida garantia de execução do contrato, nos moldes do Arts 96 a 102 da Lei nº 14.133/21, em valor correspondente a ..... % do valor total do contrato?
(X) Não

6.5. Garantia do produto/serviço, manutenção e assistência técnica
(X) Garantia e/ou assistência técnica
Especificar condições:
As condições de garantia, suporte técnico e manutenção do ecossistema unificado de segurança cibernética serão prestadas ao longo de todo o período de vigência contratual de 60 (sessenta) meses, sem qualquer custo adicional para o Município de Quatro Barras/PR, obedecendo às seguintes diretrizes técnicas e operacionais:

- **Garantia e Manutenção Corretiva de Hardware:**

Escopo: Cobertura integral contra qualquer defeito de fabricação, falha mecânica, eletromagnética ou queima de componentes dos ativos físicos fornecidos (appliances de firewall).
Modalidade On-Site: Atendimento técnico corretivo executado diretamente no Datacenter do Paço Municipal em caso de falha física que impeça o correto funcionamento do hardware.
Prazos: Diagnóstico técnico inicial em até 24 (vinte e quatro) horas após a abertura do chamado eletrônico. A substituição de peças defeituosas ou a troca integral do equipamento por um novo (ou de desempenho superior) deverá ser concluída no local em até 02 (dois) dias úteis, garantindo a manutenção da redundância do cluster em Alta Disponibilidade.

- **Manutenção Preventiva e Evolutiva Lógica:**

Escopo: Fornecimento contínuo e automatizado de atualizações lógicas e correções de SOFTWARE emitidas diretamente pelos fabricantes das soluções.
Ações Obrigatórias: Atualização diária e em tempo real de assinaturas de vírus, vacinas contra RANSOMWARES, banco de dados de reputação de IPS/URL e vacinas do sistema de prevenção de intrusões (IPS), além da aplicação imediata de patches de segurança para mitigar vulnerabilidades de "dia zero".

- **Assistência Técnica Especializada e Monitoramento (SOC 24x7x365):**

Escopo: Operação remota, triagem de telemetria de logs, ajuste de políticas e intervenção proativa em caso de incidentes, executada por equipe técnica vinculada ao Centro de Operações de Segurança (SOC).
Acordo de Nível de Serviço (SLA): Os chamados lógicos abertos pela fiscalização ou detectados automaticamente pelo SOC deverão cumprir os seguintes tempos limites de atendimento e contenção definitiva:

- Severidade Altíssima: Atribuição em até 30 minutos; primeiro diagnóstico em até 1 hora; resolução e contenção final do evento em até 4 horas (período 24x7x365).
- Severidade Alta: Atribuição em até 1 hora; primeiro diagnóstico em até 2 horas; resolução e contenção final em até 6 horas (período 24x7x365).
- Severidade Média: Atribuição em até 1 hora; primeiro diagnóstico em até 26 horas; resolução e contenção final em até 12 horas (período 24x7x365).
- Severidade Baixa / Consulta: Atendimento em conformidade com as rotinas administrativas e operacionais de TI.

7.OBRIGAÇÕES ESPECÍFICAS DAS PARTES

7.1 Da contratada

Obriga-se a empresa vencedora:
a) Atender a todas as solicitações de contratação efetuadas durante a vigência do Contrato, limitada ao quantitativo de cada item;
b) Executar o fornecimento e a prestação dos serviços de acordo com as especificações constantes no Edital e no Termo de Referência, em estrita consonância com a proposta apresentada e com a qualidade e especificações determinadas pela legislação em vigor;
c) Responsabilizar-se pela boa execução e eficiência na entrega dos produtos e prestação dos serviços objeto do edital;
d) Reparar, corrigir e remover às suas expensas, no todo ou em parte, os objetos em que se verifiquem danos ou vícios em decorrência do transporte, fabricação ou instalação, providenciando a imediata substituição dos mesmos;
e) Providenciar a imediata correção das deficiências apontadas pelo Contratante quando da execução do serviço ou fornecimento dos bens;
f) Não subcontratar, ceder ou transferir, total ou parcialmente, o objeto do contrato;
g) Manter, durante toda a vigência do contrato (60 meses), todas as condições de habilitação jurídica, qualificação técnica e regularidade fiscal e econômico-financeira exigidas na licitação;
h) Estender ao contrato os benefícios e promoções oferecidos aos demais clientes da Contratada;
i)Responsabilizar-se por quaisquer danos ou prejuízos físicos ou materiais causados à Administração ou a terceiros, por seus prepostos, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança, quando da execução do fornecimento/serviço;
j) Responsabilizar-se por todas e quaisquer despesas, de natureza previdenciária, fiscal, trabalhista ou civil, bem como emolumentos, ônus ou encargos de qualquer espécie e origem, pertinentes à

execução do objeto contratado, eximindo o Município de Quatro Barras de qualquer solidariedade jurídica;
k) Manter endereço eletrônico (e-mail) válido para fins de comunicação com o Contratante por todo o período de contratação, comunicando imediatamente caso ocorra alteração;
l) Efetuar a entrega, montagem em rack (máximo de 3U para os Firewalls e 2U para o Servidor de Logs), cabeamento e ativação elétrica dos ativos físicos fornecidos no Datacenter Central da Prefeitura, garantindo o funcionamento imediato do arranjo de Alta Disponibilidade (Cluster Ativo-Passivo);
m) Realizar o mapeamento e a migração integral da matriz de regras de firewall, rotas, políticas de segurança e acessos vigentes na prefeitura, sem causar interrupções nos serviços públicos essenciais (saúde, arrecadação, segurança) ou nos sistemas de telefonia VoIP;
n) Disponibilizar e auxiliar tecnicamente a equipe local na instalação e homologação dos agentes de software para a proteção avançada dos endpoints (estações e servidores) e na ativação da plataforma de nuvem para os usuários de Autenticação Multifator (MFA);
o) Fornecer à Diretoria de TIC, no prazo máximo de 30 (trinta) dias úteis após a instalação, o documento técnico completo contendo o mapeamento lógico e a topologia final da solução em formato digital;
p) Prestar manutenção corretiva nos appliances físicos com fornecimento de peças e mão de obra inclusos. A substituição de peças defeituosas ou do hardware danificado deve ser concluída no local em até 02 (dois) dias úteis após a abertura do chamado;
q)Assegurar o fluxo contínuo e diário de atualizações de assinaturas de vírus, base de dados de IPS, reputação de URLs e correções de segurança emitidas diretamente pelo fabricante;
r) Operar o Centro de Operações de Segurança (SOC) de forma ininterrupta (24x7x365), garantindo o cumprimento rígido dos Acordos de Nível de Serviço (SLA) acordados, com destaque para o tempo máximo de até 4 horas para a contenção e resolução definitiva de incidentes de criticidade Altíssima;
s) Emitir mensalmente à fiscalização do contrato relatórios consolidados em formato digital detalhando todos os alertas triados, tentativas de intrusão bloqueadas, vulnerabilidades corrigidas nos endpoints e o índice de cumprimento de SLA;
t) Ministrar treinamento técnico oficial com carga horária mínima de 24 (vinte e quatro) horas, voltado à capacitação dos servidores/técnicos da prefeitura, fornecendo materiais didáticos digitais, certificados e os vouchers para certificação oficial do fabricante;
u) Responsabilizar-se integralmente pelo recolhimento, transporte e descarte ecologicamente correto de todas as peças, componentes ou hardwares substituídos ou desativados ao longo do contrato, cumprindo as diretrizes da Diretiva RoHS e as normas de proteção ambiental vigentes;
v) Manter absoluto sigilo sobre quaisquer dados lógicos, credenciais, topologias de rede ou informações pessoais às quais tiver acesso em decorrência do monitoramento e execução do objeto, cumprindo rigorosamente as disposições da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018).

7.2 Da contratante
Obriga-se a Administração/Contratante:
a)comunicar a Contratada toda e quaisquer ocorrências relacionadas aos objetos entregues;
b)efetuar o pagamento da Contratada de acordo com a forma de pagamento estipulada na licitação e no Contrato;
c)promover o acompanhamento e a fiscalização do fornecimento/prestação dos serviços, sob os aspectos qualitativo e quantitativo, anotando em registro próprio as falhas e solicitando as medidas corretivas;
d)rejeitar, no todo ou em parte, o objeto entregue pela Contratada fora das especificações do contrato;
e)observar para que durante a vigência do Contrato sejam cumpridas as obrigações assumidas pela Contratada, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas na licitação;
f)aplicar as sanções administrativas, quando se fizerem necessárias;
g)prestar à CONTRATADA informações e esclarecimentos que venham a ser solicitados;
h)demais condições constantes do edital de licitação.

8.DO CONTRATO
8.1.INSTRUMENTO CONTRATUAL

(X) Somente por assinatura de contrato

A formalização da contratação dar-se-á obrigatoriamente por meio da celebração de Termo de Contrato, nos moldes do art. 95, *caput*, da Lei Federal nº 14.133/2021. A substituição do instrumento contratual por carta-contrato, nota de empenho ou autorização de fornecimento é inviável no presente caso, tendo em vista a alta complexidade do objeto, o horizonte temporal de execução continuada fixado em 60 (sessenta) meses, a necessidade de fixação de obrigações contratuais complexas de sigilo/LGPD, a vinculação a regramento estrito de sanções administrativas e o acompanhamento de metas rígidas de Acordos de Nível de Serviço (SLA) para a operação e monitoramento do Centro de Operações de Segurança (SOC 24x7x365).

8.2.VIGÊNCIA

(X) O prazo de vigência da contratação é de 60 (sessenta) meses, contados da data de assinatura do contrato, prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

8.2.1 Se foi definida vigência plurianual, justifique:

A definição do prazo de vigência inicial de 60 (sessenta) meses fundamenta-se nas diretrizes da Lei Federal nº 14.133/2021 e nos estudos do ETP:

Enquadramento Legal (Artigo 106 da Lei nº 14.133/2021): O objeto abrange a prestação de serviços continuados de monitoramento, triagem e resposta a incidentes por meio do Centro de Operações de Segurança (SOC 24x7x365), além do fornecimento ininterrupto de subscrições lógicas de segurança (atualizações diárias de vacinas e assinaturas de ameaças). A interrupção dessa blindagem digital comprometeria a continuidade das atividades essenciais do Município (como saúde, arrecadação e segurança) e o cumprimento das exigências da LGPD, configurando-se como necessidade permanente e contínua.

Vantajosidade Econômica e Amortização: A vigência plurianual de 5 anos permite a diluição e a amortização dos custos operacionais e de engenharia iniciais (instalação física, cabeamento, migração da matriz de regras de rede e treinamento da equipe de TIC). Além disso, blinda o erário municipal contra variações cambiais no mercado de tecnologia, garantindo preços estáveis e previsibilidade orçamentária para a Administração ao longo de todo o período.

8.3.GESTÃO E FISCALIZAÇÃO

Gestor:

Nome: Viviane Sautner Bernardi
Cargo: Secretária Municipal
Matrícula: 8654

Fiscal:

Nome: Alessandro Cordeiro Blanco
Cargo: Coordenador de Departamento
Matrícula: 8937

9.CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

9.1 Prazos

Prazo de pagamento do documento fiscal: regulamentada pelo Decreto Municipal n° 10.279/2024, esse prazo total máximo é de 30 (trinta) dias úteis.

Atendendo ao decreto de n° 11.925/2026, Recebimento Provisório: Ocorre em até 03 (três) dias úteis após a comunicação formal do fornecimento e entrega física/lógica pela Contratada. Recebimento Definitivo: Ocorre em até 15 (quinze) dias úteis contados a partir do recebimento provisório.

10.DA DOTAÇÃO ORÇAMENTÁRIA

As despesas correrão a conta da dotação:

Órgão	Código Reduzido	Subação	Natureza	Fonte
03.001	20	03.001.04.122.0002.2.008.3.3.90.40.00.00	Serviços de TIC – PJ	1000 – Recurso livre
03.003	56	03.003.04.126.0025.2.211.3.3.90.40.00.00	Serviços de TIC – PJ	1000 – Recurso livre
04.003	151	04003219000080244003433904000000	Serviços de TIC – PJ	1000 – Recurso livre

06.001	223	06001103010012207633904000000	Serviços de TIC – PJ	1303 – Recurso livre
25.002	566	25002123650018203933904000000	Serviços de TIC – PJ	1103 - Recurso livre
25.002	567	2500212365001820393390400000	Serviços de TIC – PJ	1104 - Recurso livre
25.003	598	25003123610017203933904000000	Serviços de TIC – PJ	1103 - Recurso livre

11.INFORMAÇÕES ADICIONAIS

11.1. Vinculação e Descrição Completa dos Itens da Solução

Integra o presente Termo de Referência, para todos os fins de direito e obrigações contratuais, a descrição detalhada e exaustiva de cada um dos componentes do ecossistema de segurança cibernética constante neste termo.

O objeto compõe-se de Lote Único contendo os seguintes itens e serviços cujas especificações de desempenho, portas, arquitetura e funcionalidades lógicas obedecem estritamente:

1. **Item 1:** Firewall de Próxima Geração (NGFW em Alta Disponibilidade - HA - 2 Unidades);
2. **Item 2:** Solução de Centralização, Retenção e Análise de Logs (Máquina Virtual - 1 Unidade);
3. **Item 3:** Proteção Avançada para Estações de Trabalho (EPP e ZTNA - 600 Licenças);
4. **Item 4:** Gestão Segura de Identidade e Autenticação Multifator (MFA/SSO - 100 Usuários / 40 Soft Tokens);
5. **Item 5:** Solução de Gerenciamento de Acesso Privilegiado (PAM - 5 Serviços / até 45 Agentes);
6. **Item 6:** Serviço de Transferência de Conhecimento e Capacitação Técnica (5 Serviços / Treinamento de 24h + 4 Vouchers de Certificação);
7. **Item 7:** Serviços de Implantação Física, Lógica e Migração de Regras (9 Serviços).

11.2. Índices e Matriz de Medição de Acordos de Nível de Serviço (SLA)

A prestação dos serviços continuados de suporte, manutenção preventiva/corretiva e monitoramento proativo via Centro de Operações de Segurança (SOC) operando em regime de 24 horas por dia, 7 dias por semana e 365 dias por ano (24x7x365) estará vinculada às seguintes metas e prazos máximos de atendimento e contenção definitiva:

Criticidade do Chamado	Tempo Máximo de Atribuição	Tempo Máximo para 1º Diagnóstico	Tempo Máximo para Resolução e Contenção Definitiva	Regime de Cobertura
Severidade Altíssima *(Indisponibilidade de serviços críticos, ataque ativo ou ransomware)*	Até 30 minutos	Até 1 hora	Até 4 horas	24x7x365
Severidade Alta *(Comprometimento parcial de regras de segurança sem parada geral)*	Até 1 hora	Até 2 horas	Até 6 horas	24x7x365
Severidade Média *(Instabilidades pontuais ou falhas em componentes redundados)*	Até 1 hora	Até 26 horas	Até 12 horas	24x7x365
Severidade Baixa / Consulta *(Dúvidas operacionais, suporte administrativo ou pequenas alterações)*	Conforme rotina	Conforme rotina	Prazos operacionais de TI	Horário Comercial

Manutenção e Substituição Física de Hardware: O diagnóstico técnico para chamados decorrentes de falhas físicas no equipamento deverá ser emitido em até 24 (vinte e quatro) horas. A substituição física de peças defeituosas ou a troca integral do equipamento danificado no Datacenter do Paço Municipal deverá ocorrer no prazo máximo de até 02 (dois) dias úteis.

11.3. Das Infrações e Sanções Administrativas

Em estrita observância ao Título IV da Lei Federal nº 14.133/2021 e visando resguardar a rede municipal contra falhas operacionais ou descontinuidade da proteção, a Contratada estará sujeita às seguintes penalidades, garantido o devido processo administrativo e o contraditório:

1. **Advertência:** Aplicável em casos de descumprimento leve de obrigações contratuais que não causem impacto direto na disponibilidade ou na segurança lógica dos dados do Município.

2. **Multas Moratórias e Compensatórias:** Atraso na Entrega e Implantação Inicial: Multa diária de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor total estimado para a fase de instalação, limitada a 20 dias úteis. Passados 20 dias, configurará inexecução parcial do objeto.
3. **Descumprimento Geral de Obrigações:** Multa de 5% (cinco por cento) por infração a qualquer obrigação descrita na Cláusula de Obrigações da Contratada que não possua penalidade específica.
4. **Inexecução Parcial ou Total do Contrato:** Multa compensatória de 15% (quinze por cento) sobre o valor global do contrato, caso a empresa dê causa à rescisão administrativa.
5. **Multas Específicas e Glosas por Quebra de SLA (SOC 24x7x365):** Quebra de SLA de Severidade Altíssima (Teto de 4 horas): Glosa/multa de 2% (dois por cento) por hora extra ou fração de hora de atraso na contenção do incidente, limitada ao teto de 10% do valor da fatura mensal por ocorrência. Quebra de SLA de Severidade Alta (Teto de 6 horas): Glosa/multa de 1% (um por cento) por hora extra ou fração de hora de atraso, limitada a 5% por ocorrência. Indisponibilidade do Cluster de Firewall: Caso o arranjo de Alta Disponibilidade (HA) falhe por completo e cause a interrupção geral do tráfego da rede por culpa imputável à Contratada, aplicar-se-á multa automática de R$ 5.000,00 por hora de paralisação, cumulada com a abertura de processo de suspensão.
6. **Impedimento de Licitar e Contratar e Declaração de Inidoneidade:** Impedimento (Art. 156, III): Prazo de até 3 (três) anos aplicável às empresas que apresentarem documentação falsa, retardarem a licitação ou praticarem atos fraudulentos. Inidoneidade (Art. 156, IV): Prazo de 3 (três) a 6 (seis) anos aplicável a fraudes graves, conluios ou vazamento culposo/doloso de dados do Município (LGPD).

11.4. Diretrizes Técnicas Complementares e Sustentabilidade

Arquitetura Baseada em Nuvem (SaaS): As subscrições lógicas de Proteção de Endpoints (EPP/ZTNA) e o sistema de Autenticação Multifator (MFA) deverão operar obrigatoriamente sob a arquitetura de Software como Serviço (SaaS), com console de gerência hospedada em nuvem pública/privada de alta disponibilidade, desonerando a infraestrutura física de servidores internos da Prefeitura.

Sustentabilidade Ambiental e Eficiência Energética: Em atendimento às normas ambientais e ao Guia de Contratações Sustentáveis do TCE/PR, os componentes de hardware fornecidos deverão possuir certificação de eficiência energética. Adicionalmente, toda a documentação gerada ao longo do contrato deverá ser gerada e armazenada de forma exclusivamente digital.

Alinhamento com Contratos Correlatos de TIC: As parametrizações lógicas e a matriz de roteamento do Firewall deverão suportar e integrar-se perfeitamente aos sistemas legados de telefonia fixa e móvel do Município (STFC/VoIP), mantendo total compatibilidade com a rotina de infraestrutura exercida pelos técnicos locais e pelo suporte terceirizado de TI.

Loana Cavalli da Conceição
Responsável pela elaboração do Termo de Referência

Viviane Sautner Bernardi
Secretária Municipal de Administração, Finanças e Planejamento

ANEXO 02
ESTUDO TÉCNICO PRELIMINAR

A contratação tem por objeto a escolha de empresa especializada para o fornecimento de uma solução integrada e centralizada de segurança cibernética e gestão segura de identidades.

1.INTRODUÇÃO

1.1. O presente documento caracteriza a primeira etapa da fase de planejamento e apresenta os devidos estudos para a contratação de solução que atenderá à necessidade abaixo especificada. O objetivo principal é estudar detalhadamente a necessidade e identificar no mercado a melhor solução para supri-la, em observância às normas vigentes e aos princípios que regem a Administração Pública.

2.INFORMAÇÕES GERAIS

2.1. Secretaria solicitante: Secretaria Municipal de Administração, Finanças e Planejamento – Departamento de Tecnologia da Informação, para atender as demais secretarias municipais.
2.2. Objeto: A contratação tem por objeto a escolha de empresa especializada para o fornecimento de uma solução integrada e centralizada de segurança cibernética e gestão segura de identidades.

3.DESCRIÇÃO DA NECESSIDADE

3.1. A presente contratação visa suprir a necessidade de proteção integral, modernização e monitoramento da infraestrutura tecnológica da Prefeitura Municipal de Quatro Barras. O problema a ser resolvido consiste na mitigação dos crescentes riscos cibernéticos e vazamento de dados, que ameaçam a continuidade de serviços públicos essenciais prestados aos cidadãos. Sob a perspectiva do interesse público, a contratação garante a disponibilidade contínua dos serviços digitais, a salvaguarda das informações institucionais e o estrito cumprimento da Lei Geral de Proteção de Dados (LGPD).
3.2. Lei Federal nº. 14.133, de 1º de abril de 2021, com ênfase nos princípios da eficiência, segurança jurídica, economicidade e na busca pela proposta mais vantajosa para a Administração Pública.
3.3. A demanda originou-se da necessidade de estruturar um ecossistema de segurança da informação robusto e integrado para a rede municipal. O cenário tecnológico atual exige ferramentas que operem de forma coordenada, visto que soluções fragmentadas apresentam ineficiência no combate a ameaças modernas.
Os principais problemas e necessidades identificados que justificam a contratação incluem:

- Necessidade de proteção avançada do perímetro da rede e dos dispositivos, prevenindo ataques que possam causar indisponibilidade nos sistemas de gestão, saúde e telefonia VoIP do município.
- Ausência de resposta imediata a incidentes fora do horário de expediente, o que fundamenta a necessidade de um Centro de Operações de Segurança (SOC) atuando em regime 24x7x365.
- Necessidade de garantir a autenticidade dos acessos aos sistemas críticos por meio de Autenticação Multifator (MFA), Acesso Seguro Baseado em Zero Trust (ZTNA) e Gerenciamento de Acesso Privilegiado (PAM), assegurando a proteção de dados sensíveis.
- Necessidade de que os ativos perimetrais atuem em cluster de alta disponibilidade, evitando que falhas de hardware paralisem a comunicação do município.
- O processo atual é fruto da revisão de um certame anterior (Pregão 50/2026), revogado justamente para aperfeiçoar as especificações técnicas (desempenho, escalabilidade, continuidade) e a arquitetura da solução, garantindo a integração nativa dos componentes e o melhor aproveitamento dos recursos públicos.

4.ESTIMATIVA DA QUANTIDADE DE BENS E SERVIÇOS

4.1. A contratação foi agrupada em lote único, contemplando a solução integrada de segurança cibernética e gestão segura de identidades, com vigência de 60 meses. Esse agrupamento possibilita a economia de escala, reduz a fragmentação administrativa e assegura a interoperabilidade nativa entre as soluções de borda e de endpoints.
As quantidades estimadas para a contratação são as seguintes:

- Item 1: Firewall de Próxima Geração (NGFW) - 2 unidades.

- Item 2: Solução de centralização e armazenamento de logs (Máquina Virtual) - 1 unidade.
- Item 3: Licenciamento de Proteção Avançada (EPP) e Acesso Seguro (ZTNA) - 600 licenças.
- Item 4: Solução de Autenticação Multifator (MFA) e Gestão de Identidade - 100 licenças.
- Item 5: Solução de Gerenciamento de Acesso Privilegiado (PAM) - 45 licenças (para agentes).
- Item 6: Serviços de Treinamento e Certificação Técnica - 5 serviços (lote de capacitação para até 10 profissionais e 4 vouchers de certificação).
- Item 7: Serviços de Implantação Física e Lógica - 9 serviços (etapas de migração e ativação).

4.2. Considerando que esta é a primeira compra destas soluções integradas de segurança cibernética pelo Município, não há um perfil de consumo ou histórico de contratações anteriores idênticas que sirvam de base. Dessa forma, as quantidades não foram baseadas em consumo passado, mas sim estimadas em função da provável utilização, tendo como métricas o dimensionamento do parque tecnológico atual e as melhores práticas de arquitetura de rede para a implementação inicial do projeto:

- Firewall NGFW (2 unidades): Quantidade mínima e exata para estabelecer a arquitetura de Alta Disponibilidade (*High AVAILABILITY* - HA) em modo ativo-passivo. Sendo a primeira implantação dessa robustez, é imprescindível ter um equipamento redundante para assumir o tráfego em caso de falha do principal, garantindo a continuidade dos serviços.
- Servidor de Logs (1 unidade): Um único servidor virtualizado é suficiente para atuar como centralizador primário dos registros de toda a rede municipal.
- EPP e ZTNA (600 licenças): A volumetria foi calculada com base no inventário atual de *endpoints* (estações de trabalho e servidores físicos/virtuais) ativos na Prefeitura, garantindo a proteção individual de cada dispositivo desde o dia zero da implantação.
- Autenticação MFA (100 licenças): O número foi projetado mapeando o contingente de usuários que possuem acesso a painéis administrativos, portais de sistemas críticos e conexões VPN, assegurando o duplo fator para essas contas sensíveis.
- Gerenciamento PAM (45 licenças): Quantidade definida pelo mapeamento restrito dos perfis de administradores de TI, terceirizados e gerentes de banco de dados que realizarão intervenções de alto nível nos servidores.
- Treinamento (5 serviços) e Implantação (9 serviços): Como a tecnologia é nova para a infraestrutura local, a implantação guiada pelo fornecedor (abrangendo montagem, migração de regras legadas e ativação lógica) e o treinamento oficial de 24 horas para até 10 servidores da Diretoria de TIC são essenciais para viabilizar o repasse da tecnologia e a autonomia operacional do Município.

4.2.1. Justificativa específica da aglutinação do Item 6 (Treinamento) no Lote Único

A inclusão do Serviço de Treinamento Técnico Oficial (Item 6) no mesmo lote dos demais componentes não decorre de mera conveniência administrativa, mas de vinculação técnica indissociável ao fornecimento dos appliances e das subscrições. O treinamento exigido é oficial do fabricante, com certificação nominal vinculada ao número de série dos equipamentos e das licenças efetivamente fornecidos ao Município. A carga horária mínima de 24 horas, o material didático oficial, a emissão dos certificados e os 4 (quatro) vouchers de certificação de nível inicial somente podem ser emitidos pelo próprio fabricante ou por seu canal oficial autorizado, por meio de plataforma de certificação atrelada à conta do cliente. A contratação isolada do treinamento por terceiro não credenciado resultaria em certificação sem validade oficial, em material desatualizado e na impossibilidade de repasse técnico adequado à equipe da Diretoria de TIC. Ademais, o treinamento é parte integrante da implantação guiada, pois é durante a instalação e a migração das regras legadas que a transferência de conhecimento se consolida. A segregação, portanto, além de não gerar economia de escala, romperia a cadeia de responsabilidade técnica única e inviabilizaria a certificação oficial exigida, razão pela qual se justifica a manutenção do Item 6 no Lote Único, nos termos do art. 47, II, da Lei nº 14.133/2021. A motivação aqui exposta atende à exigência de justificativa específica apontada pela jurisprudência do TCE/PR para a aglutinação de serviços de treinamento em lote único de soluções de TI (v.g. Acórdão nº 322/24 – Processo 253871/23).

5.ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

5.1. O valor global estimado para a contratação, referente ao período de 60 (sessenta) meses de prestação dos serviços e licenciamento, é **de R$ 2.707.575,60**. A memória de cálculo está fundamentada nas pesquisas prévias dos preços médios obtidos no mercado.

Abaixo, detalha-se a estimativa de custos por item:

Item	Descrição Resumida	Qtd	Und	Preço Médio Unitário	Total Mensal Estimado	Total Estimado (60 Meses)
1	Firewall NGFW (Hardware + Software, HA)	2	Und	R$ 8.041,10	R$ 16.082,20	R$ 964.932,00
2	Armazenamento de Logs (Máquina Virtual)	1	Und	R$ 3.498,64	R$ 3.498,64	R$ 209.918,40
3	Proteção Avançada de Estações (EPP e ZTNA)	600	Licença	R$ 18,90	R$ 11.340,00	R$ 680.400,00
4	Gestão Segura de Identidade (MFA, SSO)	1	Und	R$ 2.071,79	R$ 2.071,79	R$ 124.307,40
5	Solução de Acesso Privilegiado (PAM)	5	Serv	R$ 533,98	R$ 2.669,90	R$ 160.194,00
6	Treinamento Técnico Oficial	5	Serv	R$ 526,96	R$ 2.634,80	R$ 158.088,00
7	Implantação Física e Lógica	9	Serv	R$ 758,77	R$ 6.828,93	R$ 409.735,80
-	**TOTAL ESTIMADO**	**-**	**-**	**-**	**R$ 45.126,26**	**R$ 2.707.575,60**

5.2. A estimativa de preços preliminar foi realizada em estrita observância aos parâmetros do Decreto Municipal nº. 9618/2024. A consolidação do valor global na ordem de R$ 2,7 milhões diluídos ao longo de 60 meses comprova a viabilidade econômica do modelo de contratação em Lote Único (solução integrada como serviço), garantindo a previsibilidade orçamentária para a Secretaria Municipal de Administração e evitando oscilações inflacionárias na renovação anual de licenças pulverizadas. O orçamento estimativo final que balizará o certame passará a compor o Termo de Referência definitivo.

6.REQUISITOS DA CONTRATAÇÃO

6.1. A contratação exige uma solução tecnológica unificada de segurança cibernética que garanta a proteção do perímetro de rede, a segurança dos dispositivos (*endpoints*) e o controle de acessos, acompanhada de monitoramento proativo contínuo via Centro de Operações de Segurança (SOC) 24x7x365. A escolha recairá sobre a proposta que atender integralmente às especificações técnicas descritas no Termo de Referência, aos Acordos de Nível de Serviço (SLA) para suporte 24x7x365, à aprovação no Teste de Conformidade/Prova de Conceito (quando convocada) e à apresentação do atestado de capacidade técnica operacional compatível. A execução deverá ser acompanhada de práticas de sustentabilidade ambiental, econômica e de eficiência energética.

6.2. Requisitos necessários à contratação com vistas ao atendimento da necessidade especificada Requisitos de Habilitação Técnica Operacional e Profissional:

Atestação Técnico-Operacional: Comprovação de aptidão da empresa mediante a apresentação de no mínimo 1 (um) atestado de capacidade técnica emitido por pessoa jurídica de direito público ou privado, comprovando a execução de serviços compatíveis de Next-Generation Firewall (NGFW) em Alta Disponibilidade (HA), Endpoint Protection (EPP/ZTNA) para no mínimo 250 licenças e Autenticação Multifator (MFA) para no mínimo 40 usuários (respeitando o teto legal de até 50% do quantitativo estimado, conforme o Art. 67, § 2º, da Lei nº 14.133/2021).

Qualificação Técnico-Profissional: Comprovação de que a licitante disporá, para a fase de execução/implantação, de profissional Gerente de Projeto (com certificação PMP/MBA ou equivalente) e especialista em cibersegurança com certificação técnica no Firewall ofertado ou em cibersegurança (Art. 67, § 6º, da NLLC). Admitir-se-á a comprovação por meio de declaração de contratação futura, dispensando-se o vínculo empregatício prévio por CLT.

Afastamento de Exigências Restritivas: Em observância à jurisprudência do TCE/PR e do TCU, afasta-se a exigência de registro da empresa ou de responsáveis técnicos junto ao CREA, visto que soluções lógicas de Tecnologia da Informação não constituem atividade-fim de engenharia. Afasta-se também a obrigatoriedade de vistoria técnica presencial (substituída por Declaração de Pleno Conhecimento) e a exigência de propriedade prévia de software PAM na fase de habilitação.

7.LEVANTAMENTO DE MERCADO

7.1. O levantamento de mercado foi realizado mediante a análise do cenário tecnológico atual e a revisão das especificações do certame anterior (Pregão Eletrônico nº 50/2026, revogado para adequação técnica). A prospecção considerou a evolução das ameaças cibernéticas e as melhores práticas adotadas por outros órgãos públicos, que vêm migrando de modelos de aquisição isolada de

hardwares para a contratação de "Segurança como Serviço", garantindo monitoramento ininterrupto e integração nativa entre as plataformas.
7.2. A Administração avaliou duas abordagens principais para suprir a demanda de segurança da informação. A escolha pelo modelo integrado em lote único com serviços de SOC 24x7x365 justifica-se tecnicamente pela necessidade de automação cruzada e pela mitigação do risco de indisponibilidade. Economicamente, a gestão unificada por 60 meses elimina custos ocultos com integrações de plataformas heterogêneas e a necessidade de contratação de um grande efetivo próprio de servidores para cobrir plantões de monitoramento de madrugadas e finais de semana.
7.3. Comparativo entre as soluções existentes no mercado
Solução 1 Ecossistema Integrado de Segurança e SOC 24x7x365 (Lote Único)
Descrição completa: Fornecimento integrado de Firewalls NGFW em Alta Disponibilidade (HA), licenciamentos *Cloud* para proteção de dispositivos (EPP e ZTNA), Autenticação Multifator (MFA), Gerenciamento de Acesso Privilegiado (PAM) e Servidor de Logs, atrelados a um serviço contínuo de monitoramento proativo (SOC 24x7x365) prestado por integrador único sob Acordos de Nível de Serviço (SLA) rigorosos.
Preço Estimado: R$ 2.707.575,60 (Total para o ciclo de 60 meses).
Solução 2: Aquisição Fragmentada (Silos de Segurança) e Gestão Internalizada
Descrição completa: Aquisição de appliances físicos de firewall por meio de um processo, compra de antivírus/EPP tradicionais por outro, e gestão/monitoramento das ferramentas realizado de forma reativa e manual pela própria equipe local da Prefeitura, operando apenas em horário de expediente administrativo (8h às 17h).
Preço Estimado: Embora a compra isolada dos hardwares e licenças básicas pudesse apresentar um valor inicial inferior (estimado em R$ 1.800.000,00), o Custo Total de Propriedade (TCO) em 60 meses superaria R$ 4.500.000,00 ao se contabilizar a necessidade de nomeação ou contratação terceirizada de, no mínimo, 4 analistas seniores em regime de turno para compor um SOC interno (24x7), além dos custos de integração de sistemas de fabricantes distintos.
Conclusão do Comparativo: A Solução 1 apresenta-se objetivamente como a mais vantajosa para a Administração sob os aspectos da conveniência, economicidade e eficiência. Durante o ciclo de vida do objeto, a solução integrada transfere o ônus do monitoramento ininterrupto e da atualização tecnológica contínua para um parceiro especializado, garantindo proteção contra ataques de "dia zero" e resposta a incidentes críticos em até 4 horas. A Solução 2, além de economicamente inviável a longo prazo devido aos altíssimos custos de mão de obra especializada em cibersegurança, geraria fragilidades (falta de automação entre plataformas e monitoramento nulo fora do horário comercial), deixando o Município vulnerável a invasões noturnas e ransomwares.

8.DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

8.1. A solução definida engloba a contratação de uma plataforma integrada de segurança cibernética e gestão de identidades, fornecida no modelo de "Segurança como Serviço" pelo período de 60 meses. A infraestrutura é composta por *hardware* de proteção perimetral (Firewalls NGFW em Alta Disponibilidade), servidor de centralização de *logs*, e subscrições lógicas em nuvem para proteção de *endpoints* (ZTNA/EPP), Autenticação Multifator (MFA) e Gestão de Acessos Privilegiados (PAM).
A execução exige manutenção evolutiva (atualização contínua de vacinas, assinaturas de IPS e correções de segurança) e manutenção física on-site (substituição de peças defeituosas no Datacenter em até 2 dias úteis). A assistência técnica será prestada de forma proativa por um Centro de Operações de Segurança (SOC) operando em regime 24x7x365, sujeito a Acordos de Nível de Serviço (SLA) severos, como a exigência de contenção definitiva de incidentes críticos em até 4 horas.
A escolha deste modelo unificado (Lote Único) justifica-se tecnicamente pela capacidade de automação cruzada entre os ativos de borda e os endpoints, eliminando pontos cegos na rede e garantindo responsabilidade técnica centralizada em um único integrador em casos de incidentes. Economicamente, a opção converte altos custos de aquisição fragmentada e contratação de servidores especialistas em plantões ininterruptos em um custo operacional diluído e previsível ao longo de 5 anos, otimizando o Custo Total de Propriedade (TCO) da Administração.
8.2. Após o estudo comparativo do mercado, a solução mais vantajosa escolhida foi o Ecossistema Integrado de Segurança e SOC 24x7x365 (Lote Único**)**. Esta abordagem mostrou-se superior ao modelo tradicional de aquisição fragmentada de hardwares geridos internamente, pois garante a continuidade dos serviços públicos essenciais mesmo fora do horário de expediente, assegura o cumprimento dos preceitos da Lei Geral de Proteção de Dados (LGPD) e viabiliza a capacitação

oficial da equipe local. Esta solução, com todos os seus requisitos de desempenho, métricas de SLA, certificações exigidas e topologia, será caracterizada detalhadamente e de forma exaustiva no Termo de Referência do edital.

9.JUSTIFICATIVA DO PARCELAMENTO

9.1. A contratação não será parcelada, sendo o objeto agrupado em um Lote Único. A opção pelo não parcelamento fundamenta-se na exceção legal prevista no art. 47, inciso II, da Lei Federal nº 14.133/2021, e está alinhada à jurisprudência do Tribunal de Contas do Estado do Paraná (TCE/PR), que legitima o afastamento da regra geral de parcelamento em soluções de Tecnologia da Informação quando a divisão puder comprometer a padronização, a eficiência operacional e a segurança do ecossistema.

As justificativas técnicas e econômicas para o não parcelamento incluem:

- A eficácia da segurança cibernética moderna depende de ferramentas operando de forma coordenada e nativa. A fragmentação dos itens inviabilizaria a inteligência automatizada do ecossistema.
- A adjudicação em lote único fixa a responsabilidade jurídica e técnica sobre um único integrador. Isso elimina o risco de conflitos de responsabilidade entre diferentes fornecedores em caso de incidentes graves, garantindo o cumprimento rigoroso das metas de SLA.
- A divisão do objeto em múltiplos contratos geraria um sobrecusto de manutenção, exigiria integrações forçadas entre plataformas de fabricantes distintos e sobrecarregaria a gestão de TI, enquanto o lote único viabiliza economia de escala ao longo dos 60 meses de contrato.

  9.1.1. Inviabilidade Técnica da Integração por APIs Genéricas e Necessidade de Telemetria Nativa (SECURITY FABRIC): O agrupamento das ferramentas de Firewall (NGFW), Proteção de Endpoints (EPP/ZTNA), Centralização de Logs, Autenticação Multifator (MFA) e Gerenciamento de Acesso Privilegiado (PAM) em Lote Único não decorre de mera conveniência administrativa, mas da exigência arquitetural de resposta automatizada em tempo real (ZERO-TOUCH MITIGATION). Em um cenário de ataque ativo (como *ransomware* ou movimentação lateral), o *Endpoint* (EPP) ou o analisador de *Logs* precisa emitir instantaneamente um Índice de Comprometimento (*IOC*) e uma etiqueta de postura (*Zero Trust Tag*) que instruam o *Firewall* (NGFW) e o proxy *ZTNA* a isolar o dispositivo e revogar sessões privilegiadas (*PAM/MFA*) em milissegundos. Caso o objeto fosse parcelado entre fabricantes e fornecedores distintos, a comunicação dependeria de desenvolvimento customizado de conectores ou *APIs* abertas de terceiros — o que exige contratação adicional de fábrica de software, gera latência na contenção de ameaças, quebra a compatibilidade a cada atualização de versão (*firmware/patch*) e transfere à equipe reduzida da Prefeitura o ônus de sustentar integrações complexas. Ademais, a contratação de um Centro de Operações de Segurança (SOC 24x7x365) sob SLA rígido de contenção em até 4 horas (Item 11.2 do TR) torna-se juridicamente inexequível se houver múltiplos contratados operando camadas isoladas da mesma cadeia de defesa.

9.2. Embora os itens que compõem a solução sejam comercialmente divisíveis de forma isolada, eles são tecnicamente indivisíveis no contexto do ecossistema pretendido pela Administração. As peculiaridades de comercialização no mercado atual de segurança da informação demonstram que a contratação de "Segurança como Serviço" (MSSP) por meio de um integrador centralizado é a prática mais adequada para garantir o monitoramento ininterrupto (24x7x365) e a interoperabilidade nativa dos sistemas.

Portanto, a decisão acerca do critério de adjudicação do objeto é a de Adjudicação Global (Lote Único), visando assegurar a integridade da arquitetura de defesa cibernética do Município e a eficiência na gestão contratual.

10.CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

10.1. A partir da análise do cenário tecnológico do Município de Quatro Barras e das diretrizes fixadas no Termo de Referência, identifica-se a existência de contratações correlatas e interdependentes que exigem estrito alinhamento técnico e cooperação mútua para o sucesso da implantação da solução de segurança cibernética.

As principais interdependências identificadas englobam:

- **Contrato de Manutenção e Suporte Local de TI:** Existe interdependência direta com as rotinas de infraestrutura exercidas pelos técnicos locais e pelo Analista de Sistemas

terceirizado que atende a Prefeitura. O planejamento da futura contratação exige a articulação entre a equipe técnica da contratada do Firewall e os profissionais deste contrato de suporte de TI, garantindo o apoio presencial indispensável para a instalação em massa das licenças de Endpoint nas estações de trabalho e a homologação do ambiente.

- **Contratos de Telefonia Fixa e Móvel (STFC/VoIP):** A migração integral da matriz de regras de firewall, rotas e políticas de segurança deverá suportar e integrar-se perfeitamente aos sistemas legados de telefonia do município. É estritamente necessário planejamento para que a liberação e parametrização das políticas de telefonia VoIP não causem interrupções ou hiatos de conectividade nos serviços públicos essenciais de comunicação da administração pública.

11.ALINHAMENTO COM O PLANO DE CONTRATAÇÕES ANUAL

11.1.A presente contratação encontra-se perfeitamente alinhada ao planejamento estratégico do Município de Quatro Barras e às diretrizes da Secretaria Municipal de Administração, Finanças e Planejamento, que visam a modernização, a segurança da informação e a adequação da infraestrutura tecnológica municipal aos preceitos da Lei Geral de Proteção de Dados (LGPD).

A contratação possui previsão e adequação orçamentária confirmada, com os recursos financeiros para o pagamento das despesas já devidamente alocados nas seguintes dotações orçamentárias (fontes de recursos livres 1000, 1303, 1103 e 1104) para Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica.

12. DEMONSTRAÇÃO DOS RESULTADOS PRETENDIDOS

12.1 A contratação da solução integrada de segurança cibernética (Lote Único) projeta resultados altamente positivos e quantificáveis para a Administração Pública Municipal:

- A consolidação da contratação no valor global estimado de R$ 2.707.575,60 para um ciclo de 60 meses garante estrita previsibilidade orçamentária e blinda o Município contra oscilações inflacionárias na renovação anual de licenças. O modelo de "Segurança como Serviço" elimina o altíssimo Custo Total de Propriedade (TCO) que seria necessário para a estruturação de um Centro de Operações de Segurança (SOC) interno, o qual exigiria a contratação de, no mínimo, 4 a 5 analistas seniores em regime de turno para suprir a escala 24x7.
- A terceirização do monitoramento ininterrupto (24x7x365) desonera a equipe da Diretoria de TIC da Prefeitura da necessidade de realizar plantões de triagem de incidentes durante madrugadas e finais de semana. Ademais, a contratação engloba a capacitação e transferência de conhecimento oficial (carga horária mínima de 24 horas) para até 10 profissionais efetivos do Município, elevando o capital intelectual interno.
- A adoção de arquitetura em nuvem (*SaaS*) para o gerenciamento das 600 licenças de proteção de *endpoints* (EPP/ZTNA) e das 100 licenças de Autenticação Multifator (MFA) dispensa a aquisição, manutenção e refrigeração de novos servidores físicos no Datacenter municipal. Adicionalmente, toda a tramitação de relatórios será digital, reduzindo a zero o consumo de papel e insumos de impressão relacionados à execução contratual.

12.2. Os resultados esperados com a contratação fundamentam diretamente as métricas do Acordo de Nível de Serviço (SLA) fixadas no Termo de Referência, garantindo a continuidade dos serviços essenciais e a proteção de dados (LGPD). Os indicadores de desempenho exigidos são:

- Garantir a operação ininterrupta da rede mediante cluster de Firewalls em Alta Disponibilidade (ativo-passivo), prevendo multas automáticas em caso de interrupção geral do tráfego por culpa da contratada.
- Tempo de Resposta a Incidentes Lógicos (SOC):
    - Severidade Altíssima: Atribuição do chamado em até 30 minutos e contenção definitiva do incidente em até 4 horas.
    - Severidade Alta: Atribuição em até 1 hora e contenção definitiva em até 6 horas.
- Tempo de Reparo Físico: Realização de diagnóstico inicial em até 24 horas e substituição física de peças defeituosas ou troca do equipamento no Datacenter do Paço Municipal em até 02 (dois) dias úteis.
- Atualização e Prevenção: Atualização diária e em tempo real de assinaturas de vírus, vacinas contra ransomwares, banco de dados de reputação e políticas do IPS.

13. PROVIDÊNCIAS PRÉVIAS AO CONTRATO

13.1. Para assegurar a correta execução contratual e a rápida implantação do ecossistema de segurança cibernética, a Administração deverá executar as seguintes ações prévias:

- Assegurar que o Rack principal do Paço Municipal disponha do espaço físico necessário para a instalação (sendo reservado o máximo de 3U para os *Firewalls* e 2U para o Servidor de Logs), além de garantir refrigeração adequada e alimentação elétrica estabilizada por Nobreak com autonomia compatível para suportar oscilações.
- Promover a comunicação prévia entre os profissionais do contrato correlato de suporte de TI atual e a Diretoria de TIC, a fim de garantir o apoio logístico necessário para a instalação em massa dos agentes de Endpoint nas estações de trabalho e validação das regras de telefonia VoIP.
- Homologar e divulgar previamente, junto às demais Secretarias Municipais, o cronograma das janelas programadas de indisponibilidade extraordinária destinadas à migração física e lógica das regras de rede, mitigando impactos nos serviços de saúde, segurança e arrecadação.
- Não haverá necessidade de contratação isolada para capacitação prévia, visto que a transferência de conhecimento (treinamento oficial de 24 horas) já compõe o escopo da presente contratação. Caberá à Administração apenas a prévia indicação dos servidores da área de TI que receberão o treinamento e atuarão na administração da plataforma.

13.2. A gestão e a fiscalização do contrato serão realizadas pelos servidores designados formalmente, em conformidade com o Decreto Municipal nº 11.924/2026 e suas alterações, definidos no Termo de Referência da seguinte forma:

- **Gestora do Contrato:** Viviane Sautner Bernardi (Secretária Municipal de Administração, Finanças e Planejamento – Matrícula: 8654).
- **Fiscal do Contrato:** Alessandro Cordeiro Blanco (Coordenador de Departamento – Matrícula: 8937).

14.IMPACTOS AMBIENTAIS

14.1**.** A execução do objeto apresenta impactos ambientais potenciais relacionados ao consumo ininterrupto de energia elétrica no Datacenter municipal e à geração de resíduos eletroeletrônicos oriundos de substituições de peças.

Para mitigar esses impactos, o Termo de Referência estabelece as seguintes medidas obrigatórias:

- Os componentes de hardware fornecidos deverão possuir certificação de eficiência energética para minimizar o consumo elétrico contínuo no Datacenter.
- A Contratada é integralmente responsável pelo recolhimento, transporte e descarte ecologicamente correto de todas as peças, componentes ou hardwares substituídos ou desativados ao longo dos 60 meses de contrato, cumprindo estritamente as diretrizes da Diretiva RoHS e as normas de proteção ambiental vigentes.
- A obrigatoriedade de que os módulos de proteção de endpoints e gestão de identidades operem sob arquitetura *SaaS* (Software como Serviço) desonera a Prefeitura da necessidade de adquirir, alocar e refrigerar novos servidores físicos internos, gerando significativa economia de energia e infraestrutura.

14.2. Sob a ótica da sustentabilidade ambiental, o principal risco está atrelado ao consumo excessivo de insumos físicos (papel, toners, plásticos) para o gerenciamento de um contrato de 5 anos.

- Como ação de prevenção e contingência, o edital estipula que toda a documentação gerada ao longo do contrato (Manuais de Treinamento, Relatórios Mensais de SLA do SOC, Topologias de Rede e Atas de Reunião) deverá ser transacionada e armazenada de forma exclusivamente digital. Essa exigência de um Paperless Environment visa reduzir drasticamente a utilização de insumos de papel e impressão, alinhando-se às diretrizes do Guia de Contratações Sustentáveis do TCE/PR.

15. SERVIÇO OU FORNECIMENTO CONTÍNUO

15.1. Sim. Trata-se de serviço e fornecimento contínuo.

Justificativa: A contratação engloba a prestação de serviços de monitoramento proativo via Centro de Operações de Segurança (SOC) operando em regime ininterrupto (24x7x365), bem como o fornecimento contínuo de subscrições lógicas.

A interrupção dessa blindagem digital paralisaria e colocaria em risco atividades críticas e permanentes do Município, tais como os sistemas de saúde, segurança, arrecadação e telefonia VoIP. Portanto, por decorrer de uma necessidade prolongada e imprescindível para a manutenção da atividade administrativa e a proteção dos dados (LGPD), a contratação enquadra-se legalmente como serviço e fornecimento contínuo, permitindo o estabelecimento de um prazo de vigência inicial de 60 meses, conforme o art. 106 da Lei Federal nº 14.133/2021.

16.VIABILIDADE DA CONTRATAÇÃO

16.1. Declara-se que a presente contratação é plenamente viável, razoável e indispensável. A aquisição da solução integrada de segurança cibernética em lote único, agregada aos serviços de SOC 24x7x365, atende estritamente ao interesse público por salvaguardar os dados governamentais e garantir a continuidade da prestação de serviços essenciais à população. A modelagem adotada mitiga as inconsistências técnicas do certame anterior revogado, apresentando-se como a alternativa mais eficiente para o cumprimento das normativas da LGPD.

16.2. A análise final conclui pela adequação e viabilidade da contratação sob as seguintes dimensões:

- A solução garante proteção perimetral robusta mediante *firewalls* em Alta Disponibilidade (HA), defesa avançada de endpoints (ZTNA/EPP) e gestão segura de acessos (MFA e PAM). A automação nativa entre esses componentes assegura respostas imediatas a ataques de "dia zero" e RANSOMWARES.
- O repasse do monitoramento contínuo para um Centro de Operações de Segurança (SOC) especializado desonera a equipe de TI da Prefeitura de plantões ininterruptos. A inclusão de capacitação oficial de 24 horas garante que os servidores locais tenham autonomia para administrar o ambiente no dia a dia.
- A estimativa global de R$ 2.707.575,60 diluída ao longo de 60 meses representa um Custo Total de Propriedade (TCO) inferior à estruturação de um setor de segurança interno, além de já possuir previsão e dotação orçamentária nas fontes de recursos do Município.

Loana Cavalli da Conceição
Responsável pela elaboração do Estudo técnico preliminar

Viviane Sautner Bernardi
Secretária Municipal de Administração, Finanças e Planejamento

ANEXO 03

MODELO DE PROPOSTA DE PREÇOS

Referente: Pregão Eletrônico nº XX/2026.
Objeto: Contratação de empresa especializada para o fornecimento de solução integrada e centralizada de segurança cibernética e gestão segura de identidades, contemplando a disponibilização de ativos de segurança perimetral (firewalls em alta disponibilidade – ha), licenciamento de software para proteção avançada de dispositivos (endpoint protection), solução de autenticação multifator (mfa), bem como o fornecimento de licenças, suporte técnico, garantia e demais serviços necessários à implantação, operação e pleno funcionamento da solução

1. IDENTIFICAÇÃO DO PROPONENTE:
RAZÃO SOCIAL:
CNPJ:
REPRESENTANTE E CARGO:
CARTEIRA DE IDENTIDADE E CPF:
ENDEREÇO e TELEFONE:
AGÊNCIA e Nº DA CONTA BANCÁRIA:
ENDEREÇO ELETRÔNICO:

2. CONDIÇÕES GERAIS
2.1. A proponente declara conhecer os termos do instrumento convocatório que rege o presente processo licitatório.

3. PREÇO (READEQUADO AO LANCE VENCEDOR)

VALOR GLOBAL: R$ (por extenso).

Item	Descrição	Unidade	Quant.	Valor Unit.	Valor Total

3.1 - A validade da proposta é de 120 (cento e vinte) dias, a partir da data de abertura do pregão eletrônico.
3.2 - O preço proposto acima contempla todas as despesas necessárias a plena execução dos serviços, inclusive custos diretos e indiretos, para a perfeita execução do objeto, tais como os encargos (obrigações sociais, impostos, taxas etc.), cotados separados e incidentes sobre a execução dos serviços.
3.3 - Declaramos estar de acordo com as especificações e condições expostas no Edital e seus Anexos.

LOCAL E DATA
ASSINATURA E CARIMBO DA PROPONENTE
(OBS.: REPRESENTANTE LEGAL DA EMPRESA)

ANEXO 04

MODELO DE DECLARAÇÃO UNIFICADA

À PREFEITURA MUNICIPAL DE QUATRO BARRAS
Pregão Eletrônico n° 77/2026.

Pelo presente instrumento, a empresa (nome da empresa), inscrita no CNPJ n° (número do CNPJ), com sede na (endereço da empresa), através do seu representante legal infra-assinado, **DECLARA**, sob as penas da Lei e para fins de participação no presente certame, que:

(1) atende aos requisitos de habilitação;
(2) está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;
(3) inexiste quaisquer fatos impeditivos à sua participação na licitação, bem como que se compromete a comunicar ocorrência de fatos supervenientes;
(4) não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;
Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( )
Obs.: em caso afirmativo, assinalar a ressalva acima.

(5) não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando odisposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
(6) cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social,previstas em lei e em outras normas específicas;
(7) cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021, **no caso de licitante enquadrado como microempresa, empresa de pequeno porte ou equiparada;**
(8) está ciente sobre a observação das disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e alterações, quando do tratamento de dados pessoais e dados pessoais sensíveis a que tenha acesso, para o propósito de execução e acompanhamento do objeto licitado, não podendo divulgar, revelar, produzir, utilizar ou deles dar conhecimento a terceiros estranhos a esta contratação, a não ser por força de obrigação legal ou regulatória.

_____, em _____ de _____ de 2026.

(Assinatura do Representante Legal da Empresa Proponente).
(apontado no contrato social ou procuração com poderes específicos).

ANEXO 05
MINUTA DO CONTRATO
PREFEITURA MUNICIPAL DE QUATRO BARRAS
CONTRATO DE PRESTAÇÃO DE SERVIÇO Nº XX/XXXX
PROCESSO LICITATÓRIO Nº 77/2026 - Pregão Eletrônico
TIPO:MENOR PREÇO GLOBAL

Aos XX dias do mês de XXX de 2026, através do presente instrumento particular de **"CONTRATO DE PRESTAÇÃO DE SERVIÇO",** de um lado, o **MUNICÍPIO DE QUATRO BARRAS,** pessoa jurídica de direito público interno, inscrito no CNPJ sob nº 76.105.568/0001-39, com sede na Avenida Dom Pedro II, n° 110, nesta cidade, neste ato representado Prefeito Municipal, Senhor Loreno Bernardo Tolardo, em conjunto com a Secretária Municipal de Administração, Finanças e Planejamento Senhora Viviane Sautner Bernardi, doravante denominado "**CONTRATANTE",** e de outro lado, a empresa (NOME DA EMPRESA), pessoa jurídica de direito privado, inscrita no CNPJ sob nº (NÚMERO DO CNPJ), com sede na (ENDEREÇO DA EMPRESA), neste ato representada pelo Senhor(a) (NOME DO REPRESENTANTE), portador(a) da CI/RG nº (NÚMERO DO RG) da (ÓRGÃO EMISSOR DO RG) e inscrito no CPF/MF nº (NÚMERO DO CPF), doravante denominada "**CONTRATADA",** tem justo e convencionado o presente **CONTRATO**, atendidas as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA: "DO OBJETO"
O presente CONTRATO tem por objeto Contratação de empresa especializada para o fornecimento de solução integrada e centralizada de segurança cibernética e gestão segura de identidades, contemplando a disponibilização de ativos de segurança perimetral (firewalls em alta disponibilidade – ha), licenciamento de software para proteção avançada de dispositivos (endpoint protection), solução de autenticação multifator (mfa), bem como o fornecimento de licenças, suporte técnico, garantia e demais serviços necessários à implantação, operação e pleno funcionamento da solução, devidamente autorizado pelo Processo Licitatório de Pregão Eletrônico nº XX/2026, através do Edital e seus anexos*, que ficam fazendo parte integrante do presente em todos os seus itens e condições.

Item	Descrição	Unidade	Quant.	Valor Unit.	Valor Total

*Vinculam a esta contratação, independentemente de transcrição:
a) O Termo de Referência;
b) O Edital da Licitação;
c) A Proposta do contratado;
d) Eventuais anexos dos documentos supracitados.

§ 2º - As quantidades e os valores supra indicados são meramente estimativos de forma que os pagamentos devidos ao contratado dependerão dos quantitativos dos serviços efetivamente executados.

CLÁUSULA SEGUNDA – "DA VIGÊNCIA E PRORROGAÇÃO"
§ 1º - O prazo de vigência do contrato será de até 60 (sessenta) meses, podendo ser prorrogado na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

CLÁUSULA TERCEIRA – "DAS CONDIÇÕES DA PRESTAÇÃO DO SERVIÇO"
§ 1º - **O prazo de execução dos serviços será:**
A execução das etapas do objeto dar-se-á nos seguintes prazos, contados a partir do dia útil seguinte ao recebimento da Nota de Empenho, Ordem de Serviço ou documento equivalente:

- Até 30 (trinta) dias úteis para a entrega física de todos os ativos de hardware no Datacenter, montagem em rack, cabeamento, migração completa da matriz de regras de rede, ativação

em massa das subscrições lógicas (EPP, ZTNA, MFA e PAM) e homologação do ambiente com a entrega do relatório técnico As BUILT.

- Até 45 (quarenta e cinco) dias úteis para a conclusão e entrega do Serviço de Transferência de Conhecimento (Treinamento Técnico Oficial com carga horária mínima de 24 horas e fornecimento dos vouchers de certificação) para a equipe da Diretoria de TIC.
- 60 (sessenta) meses consecutivos para a prestação dos serviços continuados de suporte técnico, atualizações dinâmicas de segurança e monitoramento proativo via Centro de Operações de Segurança (SOC 24x7x365), contados a partir da assinatura do Termo de Recebimento Definitivo da implantação inicial.

§ 2º - **Local, horário e endereço de entrega**
Local de Entrega e Ativação Lógica: Os ativos físicos deverão ser entregues e instalados diretamente no Datacenter Central do Município, e as configurações/ativações lógicas deverão cobrir todos os computadores, servidores e usuários conectados à rede corporativa da Prefeitura Municipal de Quatro Barras/PR.
Endereço Completo: Prefeitura Municipal de Quatro Barras, Av. Dom Pedro II, nº 110 – Centro – Quatro Barras – PR, CEP 83.420-000.
Horário de Recebimento: Os bens físicos e as equipes técnicas da CONTRATADA para a instalação presencial serão recebidos exclusivamente em dias úteis, de segunda a sexta-feira, das 08h00 às 12h00 e das 13h30 às 16h30, mediante prévio agendamento com a fiscalização do contrato.
Nota Operacional: A janela de virada de chave e homologação final dos Firewalls poderá ocorrer fora do expediente tradicional (finais de semana ou madrugadas) para evitar a paralisação dos serviços públicos essenciais (saúde, arrecadação, segurança), desde que previamente acordada e autorizada pelo Departamento de TI.

§ 3º - O prazo para aceite da ordem de serviço será de até 02 (dois) dias úteis a contar da data da convocação expressa da "**CONTRATADA**".
§ 4º - Os serviços ao serem executados deverão estar em conformidade com o solicitado em edital e Termo de Referências (Anexo 01). O recebimento será feito na forma determinada pelo Decreto Municipal n° 11.925/2026.
§ 5º - Demais condições da execução dos serviços estão descritas no Anexo 01 (Termo de Referência) do referido edital.

CLÁUSULA QUARTA – "DA SUBCONTRATAÇÃO"
§ 1º - Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA: "DO VALOR E DO PAGAMENTO".
O "**CONTRATANTE**" pagará em razão dos serviços ora contratados, respeitando o valor global da contratação de R$ «Valor_Contratado».
§ 1º - Deverão ser apresentadas as notas fiscais/faturamentos nas dependências da secretaria municipal solicitante, devendo conter no corpo da nota fiscal as informações a seguir:
a) Descrição dos serviços, o número do empenho, banco, a agência bancária e o número da conta corrente para depósito do pagamento;
b) Juntamente com a nota fiscal, deverão ser apresentadas as cópias dos seguintes documentos de suporte:
b.1) certidão Negativa de Débito – CND do Instituto Nacional de Seguridade Social conjunta com a Certidão Federal - PGFN;
b.2) certificado de Regularidade do FGTS;
b.3) certificado de Regularidade dos Débitos Trabalhistas (CNDT);
b.4) certificado de Regularidade do Município (do Município sede do licitante);
b.5) cópia do empenho encaminhado para a empresa para agilizar o recebimento.
c) O prazo para o pagamento será de 30 (trinta) dias úteis em conformidade com os Decretos Municipais 9.469/2023 e 10.279/2024.
d) Quando a documentação para cobrança estiver incompleta e/ou apresentar elementos que a invalide, deverá ser substituída pela licitante, dispondo a PREFEITURA de 08 (oito) dias corridos a partir do recebimento da documentação correta, para análise e pagamento.

e) O CNPJ do estabelecimento que participar do certame, matriz/sede ou filial, deverá ser o mesmo a constar no contrato e nas Notas Fiscais/Faturas emitidas, quando da execução dos serviços contratados. Dessa forma, não será admitida a emissão de Notas Fiscais/Faturas por CNPJ de estabelecimento diverso daquele participante da Licitação.
f) Será efetuado retenção tributária prevista na legislação aplicável.
§ 2º - As despesas decorrentes da execução dos serviços, objeto do presente CONTRATO, serão suportadas com recursos da dotação orçamentária:

Órgão	Código Reduzido	Subação	Natureza	Fonte
03.001	20	03001041220002200833900400000	Serviços de TIC – PJ	1000 – Recurso livre
03.003	56	03003041260025221133900400000	Serviços de TIC – PJ	1000 – Recurso livre
04.003	151	04003219000080244003433390400000	Serviços de TIC – PJ	1000 – Recurso livre
06.001	223	06001103010012207633900400000	Serviços de TIC – PJ	1303 – Recurso livre
25.002	566	25002123650018203933900400000	Serviços de TIC – PJ	1103 - Recurso livre
25.002	567	2500212365001820393390 40000	Serviços de TIC – PJ	1104 - Recurso livre
25.003	598	25003123610017203933900400000	Serviços de TIC – PJ	1103 - Recurso livre

CLÁUSULA SEXTA – "DO REAJUSTE, REEQUILÍBRIO E REPACTUAÇÃO"
6.1 Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.
6.2 O presente contrato poderá ser objeto de reajuste, reequilíbrio e/ou repactuação, esta última exclusivamente para contratos com dedicação exclusiva de mão de obra, com o objetivo de preservar o equilíbrio-financeiro pactuado, nos termos do artigo 37, inciso XXI, da Constituição Federal, e em conformidade com os artigos 6º, inc. LVIII, 134 a 136 da Lei n° 14.133/2021.
6.2.1 Poderá ocorrer, no mesmo contrato, a aplicação concomitante de mais de um dos institutos acima descritos, desde que devidamente fundamentada e que não haja sobreposição de fatos geradores ou duplicidade de compensações.
6.3 Reajuste:
O reajuste de preços será aplicado anualmente, contado da data do orçamento estimado com base no índice IPCA ou outro que melhor reflita a variação efetiva dos custos do objeto, conforme previsto no edital e neste instrumento contratual.
6.3.1Fórmula Padrão para Aplicação de Reajuste por Índice Econômico
O reajuste será aplicado de acordo com a fórmula a seguir:

Fórmula Padrão: $VR = VO \times (1 + IVA)$

Onde:
- VR = Valor Reajustado
- VO = Valor Original (valor base do contrato ou mensal)
- IVA = Índice de Variação Acumulada, correspondente à inflação do período (em valor decimal)

Forma de cálculo do IVA:
- Quando se utiliza o índice acumulado já divulgado (ex: IPCA acumulado em 12 meses):
  IVA = percentual acumulado ÷ 100
- Quando se dispõe dos valores dos índices no início e fim do período:

6.3.2 No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE concederá à CONTRATADA a importância calculada pela última variação conhecida e a apuração da diferença ocorrerá tão logo seja divulgada a variação completa do índice.

6.3.3 Independentemente do requerimento de reajuste dos custos decorrentes do mercado, o CONTRATANTE verificará, a cada anualidade, se houve deflação do índice adotado que justifique o recálculo dos custos em valor menor, promovendo, em caso positivo, a redução dos valores correspondentes da planilha contratual.
6.3.4 Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
6.3.5 Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).
6.3.6 Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.
6.3.7 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
6.4 Reequilíbrio Econômico-Financeiro:
6.4.1 O reequilíbrio econômico-financeiro poderá ser requerido a qualquer tempo durante a execução contratual, independentemente de previsão no edital ou no contrato, quando ocorrerem fatos supervenientes à contratação que alterem substancialmente as condições iniciais pactuadas, desde que tais fatos sejam:

a) Imprevisíveis ou previsíveis, porém de consequências incalculáveis;
b) Decorrentes de caso fortuito ou força maior;
c) Resultantes de atos do Poder Público que impactem direta ou indiretamente na execução contratual (fato do príncipe).

6.4.2 - O prazo máximo para análise de pedido de reequilíbrio será de 90 dias, conforme art. 92, XI da Lei 14.133/2021.
6.4.3 O reequilíbrio econômico financeiro poderá ser solicitado tanto pela Administração quanto pela Contratada, devendo ser formalmente justificada e instruída com os documentos comprobatórios necessários, observando-se, em qualquer caso, os critérios legais e a vedação ao enriquecimento sem causa.
6.5 Repactuação
6.5.1 Os contratos com dedicação exclusiva de mão de obra ou com predominância de mão-de-obra serão repactuados mediante demonstração analítica da variação dos custos contratuais, com data vinculada:
a) à da apresentação da proposta, para custos decorrentes do mercado;
b) ao acordo, à convenção coletiva ou ao dissídio coletivo ao qual a proposta esteja vinculada, para os custos de mão de obra.

CLÁUSULA SÉTIMA – "DAS OBRIGAÇÕES DO CONTRATANTE"

a) comunicar a Contratada toda e quaisquer ocorrências relacionadas à execução do objeto contratual;
b) efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.
c) promover o acompanhamento e a fiscalização dos serviços, sob os aspectos qualitativo e quantitativo, anotando em registro próprio as falhas e solicitando as medidas corretivas;
d) rejeitar, no todo ou em parte, o serviço executado pela Contratada fora das especificações do contrato;
e) observar para que durante a vigência do Contrato sejam cumpridas as obrigações assumidas pela Contratada, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas no edital de licitação;
f) aplicar as sanções administrativas, quando se fizerem necessárias;
g) prestar à CONTRATADA informações e esclarecimentos que venham a ser solicitados;
h) demais condições constantes do edital de licitação.

CLÁUSULA OITAVA – "DAS OBRIGAÇÕES DO CONTRATADO"

a) atender a todas as solicitações de contratação efetuadas durante a vigência do Contrato, limitada ao quantitativo de cada item;
b) executar o objeto, de acordo com as especificações constantes no edital de licitação, em consonância com a proposta apresentada e com a qualidade e especificações determinadas;
c) responsabilizar-se pela boa execução e eficiência na execução do serviço;

d) reparar, corrigir, remover as suas expensas, no todo ou em parte o(s) objeto(s) em que se verifiquem danos em decorrência do transporte, bem como, providenciar a imediata substituição dos mesmos;
e) providenciar a imediata correção das deficiências apontadas pelo contratante quando da execução dos serviços;
f) apresentar, sempre que solicitado documentos que comprovem a procedência do produto/material fornecido, quando for o caso, assim como amostra para análise pela Administração, sem qualquer ônus adicional;
g) não subcontratar, ceder ou transferir, total ou parcialmente, o objeto do contrato;
h) manter, durante a vigência do contrato, todas as condições de habilitação e qualificações exigidas no edital de licitação;
i) estender ao contrato, os benefícios e promoções oferecidas aos demais clientes da contratada;
j) responsabilizar-se por quaisquer danos ou prejuízos físicos ou materiais causados à Administração ou a terceiros, pelos seus prepostos, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança, quando da execução do objeto contratual;
k) responsabilizar-se por todas e quaisquer despesas, inclusive, despesa de natureza previdenciária, fiscal, trabalhista ou civil, bem como emolumentos, ônus ou encargos de qualquer espécie e origem, pertinentes à execução do objeto contratado;
l) mesmo não sendo a fabricante da matéria prima empregada na fabricação de seus produtos/materiais, a contratada, responderá inteira e solidariamente pela qualidade e autenticidade destes, obrigando-se a substituir, as suas expensas, no todo ou em parte, o objeto da contratação, em que se verificarem vícios, defeitos, incorreções, resultantes da fabricação ou transporte, constatado visualmente ou em laboratório, correndo estes custos por sua conta;
m) manter endereço eletrônico (e-mail) válido para fins de comunicação com a contratante por todo o período de contratação, comunicando, imediatamente, o Contratante em caso de alteração;
n) Observar as demais obrigações do Termo de Referência;
o) Observar as demais condições de recebimento do Termo de Referência.
p) Efetuar a entrega, montagem em rack (máximo de 3U para os Firewalls e 2U para o Servidor de Logs), cabeamento e ativação elétrica dos ativos físicos fornecidos no Datacenter Central da Prefeitura, garantindo o funcionamento imediato do arranjo de Alta Disponibilidade (Cluster Ativo-Passivo);
q) Realizar o mapeamento e a migração integral da matriz de regras de firewall, rotas, políticas de segurança e acessos vigentes na prefeitura, sem causar interrupções nos serviços públicos essenciais (saúde, arrecadação, segurança) ou nos sistemas de telefonia VoIP;
r) Disponibilizar e auxiliar tecnicamente a equipe local na instalação e homologação dos agentes de software para a proteção avançada dos endpoints (estações e servidores) e na ativação da plataforma de nuvem para os usuários de Autenticação Multifator (MFA);
s) Fornecer à Diretoria de TIC, no prazo máximo de 30 (trinta) dias úteis após a instalação, o documento técnico completo contendo o mapeamento lógico e a topologia final da solução em formato digital;
t) Prestar manutenção corretiva nos appliances físicos com fornecimento de peças e mão de obra inclusos. A substituição de peças defeituosas ou do hardware danificado deve ser concluída no local em até 02 (dois) dias úteis após a abertura do chamado;
u) Assegurar o fluxo contínuo e diário de atualizações de assinaturas de vírus, base de dados de IPS, reputação de URLs e correções de segurança emitidas diretamente pelo fabricante;
v) Operar o Centro de Operações de Segurança (SOC) de forma ininterrupta (24x7x365), garantindo o cumprimento rígido dos Acordos de Nível de Serviço (SLA) acordados, com destaque para o tempo máximo de até 4 horas para a contenção e resolução definitiva de incidentes de criticidade Altíssima;
w) Emitir mensalmente à fiscalização do contrato relatórios consolidados em formato digital detalhando todos os alertas triados, tentativas de intrusão bloqueadas, vulnerabilidades corrigidas nos endpoints e o índice de cumprimento de SLA;
x) Ministrar treinamento técnico oficial com carga horária mínima de 24 (vinte e quatro) horas, voltado à capacitação dos servidores/técnicos da prefeitura, fornecendo materiais didáticos digitais, certificados e os vouchers para certificação oficial do fabricante;
y) Responsabilizar-se integralmente pelo recolhimento, transporte e descarte ecologicamente correto de todas as peças, componentes ou hardwares substituídos ou desativados ao longo do contrato, cumprindo as diretrizes da Diretiva RoHS e as normas de proteção ambiental vigentes;

z) Manter absoluto sigilo sobre quaisquer dados lógicos, credenciais, topologias de rede ou informações pessoais às quais tiver acesso em decorrência do monitoramento e execução do objeto, cumprindo rigorosamente as disposições da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018).
aa)Executar o fornecimento e a prestação dos serviços de acordo com as especificações constantes no Edital e no Termo de Referência, em estrita consonância com a proposta apresentada e com a qualidade e especificações determinadas pela legislação em vigor;

CLÁUSULA NONA – "DAS OBRIGAÇÕES PERTINENTES À LGPD"
§ 1º - As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.
§ 2º - Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.
§ 3º- É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.
§ 4º - A Administração deverá ser informada no prazo de 05 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.
§ 5º - Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.
§ 6º- É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.
§ 7º - O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.
§ 8º - O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.
§ 9º - O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.
§ 10º - Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.
§ 11º - Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.
§ 12º - O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.
§ 13º - Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

CLÁUSULA DÉCIMA – "DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS"
§ 1º – Comete infração administrativa a empresa e/ou a Contratada que cometer quaisquer das infrações previstas no art. 155 da Lei n°14.133/2021, quais sejam:

1 – Dar causa à inexecução parcial do contrato;
2 – Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
3 - Dar causa à inexecução total do contrato;
4 – Deixar de entregar a documentação exigida para o certame;
5 – Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
6 – Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

7 – Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
8 – Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante o certame ou a execução do contrato;
9 – Fraudar a licitação ou praticar ato fraudulento na execução do contrato;
10 – Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
a) Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quando ao enquadramento como ME/EPP ou o conluio entre os prestadores de serviço, em qualquer momento da contratação, mesmo após o encerramento da fase de lances;
11 – Praticar atos ilícitos com vistas a frustrar os objetivos do certame;
12 – Praticar ato lesivo previsto no art. 5° da Lei n° 12.846/2013.

§ 2º - Serão aplicadas ao responsável pelas infrações administrativas previstas na Lei as seguintes sanções:

a) Advertência, quando a contratada der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2°, da Lei);
b) Impedimento de licitar e contratar, quando praticadas as condutas descritas nos itens 2 a 7 do parágrafo 1°, sempre que não se justificar a imposição de penalidade mais grave (art. 156 §4°, da Lei);
c) Declaração de inidoneidade para licitar ou contratar no âmbito da Administração Pública Direta e Indireta do Ente Federativo que tiver aplicado a sanção, quando praticadas as condutas descritas nos itens 8 a 12, bem como nos itens 2 a 7 que justifiquem a imposição de penalidade mais grave (art. 156, §5, da Lei).
d) Multa:
d.1 – moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;
d.1.1 – o atraso superior a 30 (trinta) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme o disposto no inciso I, do art. 137, da Lei nº 14.133/2021.
d.2 – moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 30% (trinta por cento) pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;
d.3 – compensatória de 30% (trinta por cento) sobre o valor total do contrato, no caso de inexecução do objeto.

§ 3º – A aplicação das sanções previstas não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art.156, § 9º).
§ 4º – Todas as sanções previstas poderão ser aplicadas cumulativamente com a multa (art. 156, § 7º);

1 – Antes da aplicação da multa, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contados da data de sua intimação (art. 157);
2 – Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante a Contratada, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, § 8º);
3 – Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data de recebimento da comunicação enviada pela autoridade competente.

§ 5º – A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133/2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar e contratar.
§ 1º - Na aplicação das sanções serão considerados (art. 156 §1°):
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 a Administração Pública;
e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

§ 6º - Os atos previstos como infrações administrativas na Lei n° 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 1º de agosto de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei (art. 159).
§ 7º - A personalidade jurídica da contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos nesta Lei 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, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160).
§ 8º - Os órgãos e entidades dos Poderes Executivo, Legislativo e Judiciário de todos os entes federativos deverão, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por eles 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)
§ 9º – 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 14.133/2021.

CLÁUSULA DÉCIMA PRIMEIRA – "DA EXTINÇÃO CONTRATUAL"
§ 1º - O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.
§ 2º - O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.
§ 3º - A extinção nesta hipótese será precedida de notificação do contratado pelo contratante com pelo menos 2 (dois) meses de antecedência.
§ 4º - O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da NLLC, bem como amigavelmente, assegurados o contraditório e a ampla defesa.
1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.
2.A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará rescisão se não restringir sua capacidade de concluir o contrato.
a) Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.
§ 5º - O termo de rescisão, sempre que possível, será precedido:
1.Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;
2.Relação dos pagamentos já efetuados e ainda devidos;
3.Indenizações e multas.
§ 6º - 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).
§ 7º - 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 SEGUNDA – "DOS CASOS OMISSOS"
§ 1º - Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA TERCEIRA – "DAS ALTERAÇÕES"
§ 1º - Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

§ 2º - O CONTRATADO é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.
§ 3º - As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do termo de contrato.
§ 4º - As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos ou previsão normativa, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).
§ 5º - Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA QUARTA – "DA PUBLICAÇÃO"
§ 1º - O presente instrumento será inserido no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA DÉCIMA QUINTA – "DA FISCALIZAÇÃO"
§ 1º - Caberá aos fiscais de Contrato e aos gestores de Contrato, designados pela autoridade competente por meio do Decreto Municipal nº 11.924/2026, acompanhar e fiscalizar o cumprimento das obrigações contratuais e promover todas as ações necessárias ao fiel cumprimento do contrato.

CLÁUSULA DÉCIMA SEXTA - "DAS DISPOSIÇÕES FINAIS"
A "CONTRATADA" declara aceitar, integralmente, todos os métodos e processos de inspeção, verificação e controle a serem adotados pelo "CONTRATANTE".
§ 1º - Verificada pela fiscalização do "CONTRATANTE", o abandono do fornecimento dos produtos ou o seu retardamento indevido, poderá a mesma assumir o objeto contratual na situação em que se encontrar, constituindo os valores não pagos como créditos passíveis de cobrança por parte do "CONTRATANTE" perante a "CONTRATADA", servindo o presente CONTRATO como título executivo, na forma do disposto no art. 784, inciso II, do Código de Processo Civil.
§ 2º - Igualmente, se verificada na execução dos serviços ora contratados, a superveniência de insolvência, concordata ou falência da "CONTRATADA", serão considerados os valores não pagos como créditos privilegiados do "CONTRATANTE", podendo o mesmo prosseguir no final da execução do CONTRATO.
§ 3º - O "CONTRATANTE" reserva-se, ainda, o direito de paralisar ou suspender a qualquer tempo a execução dos serviços, mediante o pagamento único e exclusivo daqueles já entregues.
§ 4º - O "CONTRATANTE", direta ou indiretamente, fiscalizará e acompanhará a execução dos serviços.
§ 5º - No recebimento dos serviços, objeto deste CONTRATO, serão observadas as disposições estabelecidas na Lei nº 8.078 de 11.09.90 (Código de Defesa do Consumidor).

CLÁUSULA DÉCIMA SÉTIMA – "DO FORO"
Fica eleito o Foro da Comarca de QUATRO BARRAS para dirimir quaisquer questões relativas a interpretações, aplicação e execução do presente CONTRATO, renunciando as partes outro qualquer por mais privilegiado que possa ser.

E, por estarem justos e acordados, firmam o presente CONTRATO em 02 (duas) vias de igual teor e forma.

Quatro Barras, XX de XXX de 2026.

p/ CONTRATANTE:

LORENO BERNARDO TOLARDO
Prefeito Municipal

VIVIANE SAUTNER BERNARDI
Secretária Municipal de Administração, Finanças e Planejamento

p/ CONTRATADA:

Representante Legal da empresa