

PREGÃO ELETRÔNICO

06/2024
(90006/2024 no sistema compras.gov.br)

CONTRATANTE (UASG)

Câmara Municipal de Foz do Iguaçu (926470)

OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Security for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

VALOR TOTAL DA CONTRATAÇÃO

R\$ 57.310,40 (Cinquenta e sete mil, trezentos e dez reais e quarenta centavos).

DATA DA SESSÃO PÚBLICA

Dia 26/11/2024 às 10h (horário de Brasília)

CRITÉRIO DE JULGAMENTO:

Menor preço por item.

MODO DE DISPUTA:

Aberto e fechado

PREFERÊNCIA ME/EPP/EQUIPARADAS

SIM



Baixe o APP Compras.gov.br
e apresente sua proposta!



Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

Sumário

1. DO OBJETO	3
2. DA PARTICIPAÇÃO NA LICITAÇÃO	3
3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO	5
4. DO PREENCHIMENTO DA PROPOSTA	6
5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES.....	7
6. DA FASE DE JULGAMENTO	10
7. DA FASE DE HABILITAÇÃO.....	11
8. DOS RECURSOS	13
9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES	14
10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO	16
11. DAS DISPOSIÇÕES GERAIS	16





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU

PREGÃO ELETRÔNICO Nº 05/2024.

(Processo Administrativo IDOC nº279/2024)

Torna-se público que a Câmara Municipal de Foz do Iguaçu, por meio do Setor de Compras, sediada na Travessa Oscar Muxfeldt, nº 81, Centro, Foz do Iguaçu – PR, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da [Lei nº 14.133, de 1º de abril de 2021](#), do Atos da Presidência nº [131/2023](#) e nº [134/2023](#) demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Security for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

1.2. A licitação será realizada em item único.

ITEM	DESCRIÇÃO	BENEFÍCIO ME/EPP	QNT	VALOR UNITÁRIO	VALOR TOTAL
1	Licença KASPERSKY NEXT EDR OPTIMUM 36 meses	Tratamento favorecido	160	R\$ 358,19	R\$ 57.310,40

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

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

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

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

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto nº 8.538, de 2015, bem como para bens e serviços





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

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

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

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

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

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

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

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

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

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

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

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da [Lei nº 14.133/2021](#).

2.12. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.11.1 deste Edital.

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

3.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas 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;

3.4.2. 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 7º, XXXIII, da Constituição](#);

3.4.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos [incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal](#);

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

3.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 16 da Lei nº 14.133, de 2021](#).

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

3.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.6.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 3.7. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na [Lei nº 14.133, de 2021](#), e neste Edital.
- 3.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.
- 3.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.
- 3.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.
- 3.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:
- 3.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e
 - 3.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.
- 3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:
- 3.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e
 - 3.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.
- 3.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.
- 3.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.
- 3.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

- 4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:
- 4.1.1. Valor unitário e total do item;
 - 4.1.2. Marca;
 - 4.1.3. Fabricante;
 - 4.1.4. Quantidade cotada, devendo respeitar o mínimo para cada item.
- 4.2. Todas as especificações do objeto contidas na proposta aceita pela Administração vinculam o licitante.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 4.2.1. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao previsto para a contratação.
- 4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.
- 4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.
- 4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.
- 4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.
- 4.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, quando devidamente aceita pela administração, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.
- 4.7.1. O prazo de validade da proposta **não será inferior a 90 (noventa)** dias, a contar da data de sua apresentação, independentemente do prazo indicado no documento encaminhado.
- 4.7.2. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;
- 4.8. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do [art. 71, inciso IX, da Constituição](#); ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

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

- 5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.
- 5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.
- 5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.
- 5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.
- 5.5. O lance deverá ser ofertado pelo valor unitário do item
- 5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.
- 5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.
- 5.8. O intervalo mínimo de diferença de valores, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R\$ 1,00 (Um real).





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexecutável.
- 5.10. O procedimento seguirá de acordo com o modo de disputa aberto e fechado.
- 5.11. Para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.
- 5.11.1. 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.
- 5.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.
- 5.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.
- 5.11.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.
- 5.11.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.
- 5.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.
- 5.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
- 5.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.
- 5.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.
- 5.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.
- 5.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.
- 5.18. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.
- 5.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 5.18.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.
- 5.18.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.
- 5.18.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.
- 5.19. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.
- 5.19.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no [art. 60 da Lei nº 14.133, de 2021](#), nesta ordem:
- 5.19.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;
- 5.19.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;
- 5.19.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;
- 5.19.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.
- 5.19.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:
- 5.19.2.1. empresas estabelecidas no território do Estado do Paraná;
- 5.19.2.2. empresas brasileiras;
- 5.19.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;
- 5.19.2.4. empresas que comprovem a prática de mitigação, nos termos da [Lei nº 12.187, de 29 de dezembro de 2009](#).
- 5.19.3. Se, mesmo após a aplicação dos procedimentos previstos nos itens acima, ainda persistir o empate, será realizado sorteio público para fins de desempate;
- 5.19.3.1. Será informado no chat da sessão pública, a data, hora e local do sorteio, a ser realizado no site [sorteio.com](#) (ou outro compatível), com transmissão ao vivo no Youtube ou outra plataforma de streaming;
- 5.19.3.2. Haverá lavratura de ata de sorteio, com presença de testemunhas, que será incluída no processo administrativo.
- 5.20. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro deverá negociar condições mais vantajosas, após definido o resultado do julgamento.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 5.20.1. Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo.
- 5.20.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.
- 5.20.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
- 5.20.4. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.
- 5.20.5. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.
- 5.20.6. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.
- 5.21. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

- 6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no [art. 14 da Lei nº 14.133/2021](#), legislação correlata e no item 2.5 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:
- 6.1.1. SICAF;
- 6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>); e
- 6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>).
- 6.1.4. Cadastro de restrições ao direito de contratar com a Administração Pública (<https://crcap.tce.pr.gov.br/ConsultarImpedidos.aspx>)
- 6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o [artigo 12 da Lei nº 8.429, de 1992](#).
- 6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.
- 6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.
- 6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.
- 6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.
- 6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5.1 e 4.6 deste edital.

6.6. Verificadas as condições de participação, o pregoeiro examinará a proposta final ajustada, ofertada pela empresa classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no [artigo 27 a 33 do Ato da Presidência nº 134/2023](#).

6.7. Será desclassificada a proposta vencedora que:

- 6.7.1. contiver vícios insanáveis;
- 6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;
- 6.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;
- 6.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;
- 6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

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

6.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

- 6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e
- 6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.8.2. Será desclassificada a proposta que não tiver sua exequibilidade demonstrada, quando exigido pela Administração.

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

6.10. 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.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos neste item, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos [arts. 62 a 70 da Lei nº 14.133, de 2021](#).

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

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

7.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

juramentado no País e apostilados nos termos do disposto no [Decreto nº 8.660, de 29 de janeiro de 2016](#), ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou original e cópia simples para autenticação pela Equipe de Pregão e posterior devolução.

7.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

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

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

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

7.9. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. ([IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º](#)).

7.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. ([IN nº 3/2018, art. 7º, caput](#)).

7.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. ([IN nº 3/2018, art. 7º, parágrafo único](#)).

7.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de DUAS HORAS, prorrogável por igual período, contado da solicitação do pregoeiro.

7.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.12.1. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para ([Lei 14.133/21, art. 64](#), e [Ato da Presidência nº 134/2023, art. 35, §4º](#)):

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

7.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 7.14. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.
- 7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.
- 7.16. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.
- 7.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).
- 7.18. Serão exigidos os seguintes documentos para a habilitação:
- 7.18.1. Habilitação jurídica nos termos do art. 66 da Lei nº 14.133/2021;
 - 7.18.2. Prova da inexistência de fato impeditivo para licitar ou contratar com a Administração Pública, mediante a juntada de pesquisa realizada junto ao Tribunal de Contas da União e ao Tribunal de Contas do Estado do Paraná;
 - 7.18.3. Habilitação fiscal, social e trabalhista, nos termos do Art. 68 da Lei nº 14-133/2021;
 - 7.18.4. Habilitação econômico-financeira, mediante o fornecimento de Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante;

8. DOS RECURSOS

- 8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.
- 8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.
- 8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:
- 8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;
 - 8.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.
 - 8.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;
- 8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.
- 8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.
- 8.6. Os recursos interpostos fora do prazo não serão conhecidos.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.
- 8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.
- 8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.
- 8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico <https://www.fozdoiguacu.pr.leg.br/transparencia/licitacoes/2024/pregao-eletronico-006-2024/>

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

- 9.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:
- 9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;
- 9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não manter a proposta em especial quando:
- 9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;
- 9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;
- 9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou
- 9.1.2.4. deixar de apresentar amostra;
- 9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;
- 9.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- 9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;
- 9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação
- 9.1.5. fraudar a licitação
- 9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:
- 9.1.6.1. agir em conluio ou em desconformidade com a lei;
- 9.1.6.2. induzir deliberadamente a erro no julgamento;
- 9.1.6.3. apresentar amostra falsificada ou deteriorada;
- 9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação
- 9.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.
- 9.2. Com fulcro na [Lei nº 14.133, de 2021](#), a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:
- 9.2.1. advertência;





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 9.2.2. multa;
- 9.2.3. impedimento de licitar e contratar e
- 9.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.
- 9.3. Na aplicação das sanções serão considerados:
- 9.3.1. a natureza e a gravidade da infração cometida.
- 9.3.2. as peculiaridades do caso concreto
- 9.3.3. as circunstâncias agravantes ou atenuantes
- 9.3.4. os danos que dela provierem para a Administração Pública
- 9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor da proposta, recolhida no prazo máximo de **15 (quinze) dias** úteis, a contar da comunicação oficial.
- 9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de **5%** do valor total da proposta.
- 9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de **30%** do valor total da proposta.
- 9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.
- 9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.
- 9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.
- 9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.
- 9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.
- 9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.
- 9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida,





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

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

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

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

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos seguintes meios: protocolo digital através do sistema 1doc através do link <https://fozdoiguacu.1doc.com.br/b.php?pg=wp/wp&itd=12> ou envio através do email licitacao@fozdoiguacu.pr.leg.br.

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

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

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

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

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

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

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

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





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 11.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.
- 11.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.
- 11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.
- 11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico <https://www.fozdoiguacu.pr.leg.br/transparencia/licitacoes/2024/pregao-eletronico-006-2024>.
- 11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:
- 11.11.1. ANEXO I - Termo de Referência
 - 11.11.2. ANEXO II – Estudo Técnico Preliminar
 - 11.11.3. ANEXO III - Minuta de Termo de Contrato
 - 11.11.4. ANEXO IV – Modelo da Proposta de Preços

JOÃO MORALES

PRESIDENTE DA CÂMARA MUNICIPAL DO IGUAÇU





Câmara Municipal de Foz do Iguaçu

TERMO DE REFERÊNCIA

1) DEFINIÇÃO DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Security for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

Item	CAT/MAT	Descrição	SKU	Quantidade total	Valor Unit.	Valor Total
<u>1</u>	350949	Licença de uso individual da solução Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R\$ 358,19	R\$ 57.310,40

2) FUNDAMENTAÇÃO DA CONTRATAÇÃO

Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da



Câmara Municipal de Foz do Iguaçu

qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em “adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

Considerando que esta casa de leis realiza a utilização da solução de segurança, sem ressalvas e visa proteger seu investimento, assegurar a padronização e compatibilidade com o ambiente computacional. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para, no mínimo, manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

Com a iminente expiração da licença, torna-se necessária a renovação e aquisição para assegurar a proteção atualizada contra as ameaças virtuais mais recentes.

Sendo a demanda prevista no PAC, conforme documento de estudo técnico preliminar - ETP.

3) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de segurança deve atender a necessidade de evolução e adequação desta casa em relação a suas ferramentas de proteção, esta casa de leis possui dois contratos ativos de licença da ferramenta KESB Select da desenvolvedora Kaspersky Global, em um deles possui o quantitativo de 130 licenças a expirar em 22/09/2024 e o outro de 20 licenças a expirar em 01/10/2024. Sendo assim, a solução apresentada deve fornecer 10 novas licenças e 150 em formato de renovação adequada à nova linha de produtos das soluções de segurança com incremento de, no mínimo EDR, bem como sua ativação. Referente a possibilidade de parcelamento, deve seguir de acordo com o ETP, por se tratar de uma solução integrada.

Custo Inicial Reduzido: Ao optar pela renovação, a empresa evita os altos custos iniciais de compra e instalação de novas soluções, permitindo a alocação de recursos para outras áreas críticas do negócio.

- **Suporte e atualizações:** Fornecimento dos serviços de suporte técnico, bem como atualizações, asseguram o perfeito funcionamento da solução.
- **Gestão Simplificada:** Por se tratar de uma solução integrada a gestão centralizada, permite aos profissionais maior autonomia e melhor condição de adaptação, visto que a equipe é reduzida.



Câmara Municipal de Foz do Iguaçu

Os itens da presente solução devem ser contratados em conjunto tendo em vista a necessidade de completa compatibilidade para o correto funcionamento.

- a) Proteção antivírus de Arquivos;
- b) Proteção antivírus da Web;
- c) Firewall local de cada máquina;
- d) Bloqueador de Ataques da Rede;
- e) Inspeção do Sistema;
- f) Inspeção avançada de dispositivos portáteis (pen drive, cartão de memória, etc);
- g) Monitoramento de Vulnerabilidades.

4) REQUISITOS DA CONTRATAÇÃO

4.1. Do módulo de proteção de endpoint

- a. A solução proposta deverá proteger os sistemas operacionais abaixo:
 - i. Windows 7
 - ii. Windows 8
 - iii. Windows 8.1
 - iv. Windows 10
 - v. Windows 11
- b. Servidores
 - i. Windows Small Business Server 2011
 - ii. Windows MultiPoint Server 2011
 - iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
- c. Servidores de terminal Microsoft
 - i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
- d. Sistemas operacionais Linux de 32 bits:
 - i. CentOS 6.7 e posterior
 - ii. Debian GNU/Linux 11.0 e posterior
 - iii. Debian GNU/Linux 12.0 e posterior
 - iv. Red Hat Enterprise Linux 6.7 e posterior
- e. Sistemas operacionais Linux de 64 bits:
 - i. Amazon Linux 2.
 - ii. CentOS 6.7 e mais tarde
 - iii. CentOS 7.2 e posterior.
 - iv. CentOS Stream 8.
 - v. CentOS Stream 9.
 - vi. Debian GNU/Linux 11.0 e posterior.
 - vii. Debian GNU/Linux 12.0 e posterior.
 - viii. Linux Mint 20.3 e superior.
 - ix. Linux Mint 21.1 e posterior.
 - x. openSUSE Leap 15.0 e posterior.
 - xi. Oracle Linux 7.3 e posterior.



Câmara Municipal de Foz do Iguaçu

- xii. Oracle Linux 8.0 e posterior.
- xiii. Oracle Linux 9.0 e posterior.
- xiv. Red Hat Enterprise Linux 6.7 e posterior
- xv. Red Hat Enterprise Linux 7.2 e posterior.
- xvi. Red Hat Enterprise Linux 8.0 e posterior.
- xvii. Red Hat Enterprise Linux 9.0 e posterior.
- xviii. Rocky Linux 8.5 e posterior.
- xix. Rocky Linux 9.1.
- xx. SUSE Linux Enterprise Server 12.5 ou posterior.
- xxi. SUSE Linux Enterprise Server 15 ou posterior.
- xxii. Ubuntu 20.04 LTS.
- xxiii. Ubuntu 22.04 LTS.
- xxiv. Sistemas operacionais Arm de 64 bits:
- xxv. CentOS Stream 9.
- xxvi. SUSE Linux Enterprise Server 15.
- xxvii. Ubuntu 22.04 LTS.
- f. Sistemas operacionais MAC OS:
 - i. macOS 12 – 14
- g. Ferramentas de virtualização MAC OS:
 - i. Parallels Desktop 16 para Mac Business Edition
 - ii. VMware Fusion 11.5 Professional
 - iii. VMware Fusion 12 Professional
- h. A solução proposta deverá suportar as seguintes plataformas virtuais:
 - i. VMware Workstation 17.0.2 Pro
 - ii. VMware ESXi 8.0 Update 2
 - iii. Microsoft Hyper-V Server 2019
 - iv. Citrix Virtual Apps e Desktop 7 2308
 - v. Citrix Provisioning 2308
 - vi. Citrix Hypervisor 8.2 Update 1

4.2. Do módulo de gerenciamento avançado

- a. A solução proposta deve suportar arquitetura cloud-native e on-premise;
- b. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
 - i. Amazon Web Services
 - ii. Microsoft Azure
- c. A solução proposta deve incluir as seguintes opções de integração SIEM:
 - i. HP (Microfoco) ArcSight
 - ii. IBM QRadar
 - iii. Splunk
 - iv. Kaspersky KUMA
- d. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
- e. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;



Câmara Municipal de Foz do Iguaçu

- f. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
- g. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
- h. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.
- i. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
- j. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.
- k. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
- l. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.
- m. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
- n. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em um único/múltiplos dispositivos com base nas seguintes regras de ativação:
 - i. Status do dispositivo
 - ii. Tag
 - iii. Diretório ativo
 - iv. Proprietários de dispositivos
 - v. Hardware
- o. A solução proposta deve suportar os seguintes canais de entrega de notificação:
 - i. E-mail
 - ii. Registro de sistema
 - iii. SMS
- p. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
 - i. Atributos de rede
 - ii. Nome
 - iii. Domínio e/ou Sufixo de Domínio
 - iv. Endereço de IP
 - v. Endereço IP para servidor de gerenciamento
 - vi. Localização no Active Directory
 - vii. Unidade organizacional
 - viii. Grupo
 - ix. Sistema operacional
 - x. Número do pacote de serviço
 - xi. Arquitetura Virtual
 - xii. Registro de aplicativos
 - xiii. Nome da Aplicação
 - xiv. Versão do aplicativo
 - xv. Fabricante



Câmara Municipal de Foz do Iguaçu

- xvi. Tipo e versão
- xvii. Arquitetura
- q. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.
- r. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.
- s. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
 - i. Dispositivos Desktop/Servidores
 - ii. Dispositivos móveis
 - iii. Dispositivos de rede
 - iv. Dispositivos virtuais
 - v. Componentes OEM
 - vi. Periféricos de computador
 - vii. Dispositivos IoT conectados
 - viii. Telefones VoIP
 - ix. Repositórios de rede
- t. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
 - i. Nome da Aplicação
 - ii. Caminho do aplicativo
 - iii. Metadados do aplicativo
 - iv. Aplicativo Certificado digital
 - v. Categorias de aplicativos predefinidas pelo fornecedor
 - vi. SHA256 e MD5
- u. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
 - i. Bluetooth
 - ii. Dispositivos móveis
 - iii. Modems externos
 - iv. CD/DVD
 - v. Câmeras e scanners
 - vi. MTPs
 - vii. E a transferência de dados para dispositivos móveis
- v. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
- w. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.
- x. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
 - i. Estruturas de domínios e grupos de trabalho do Windows
 - ii. Estruturas de grupos do Active Directory
 - iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador



Câmara Municipal de Foz do Iguaçu

- y. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.
 - z. A solução proposta deve permitir realizar as seguintes ações para endpoints:
 - i. Verificação manual;
 - ii. Verificação no acesso;
 - iii. Verificação por demanda;
 - iv. Verificação de arquivos compactados
 - v. Verificação de arquivos individuais, pastas e unidades;
 - vi. Bloqueio e verificação de scripts
 - vii. Proteção contra alteração de registros;
 - viii. Proteção contra estouro de buffer;
 - ix. Verificação em segundo plano/inativa
- 1.1. Verificação de unidade removível na conexão com o sistema;
 - 1.2. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
 - 1.3. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
 - 1.4. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
 - 1.5. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
 - 1.6. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
 - 1.7. A solução proposta deve suportar Windows Failover Cluster.
 - 1.8. A solução proposta deve ter um recurso de clustering integrado.
 - 1.9. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
 - 1.10. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
 - 1.11. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
 - 1.12. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
 - 1.13. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
 - 1.14. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
 - 1.15. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
 - 1.16. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
 - 1.17. A solução proposta deverá possuir controles para download de DLL e drivers.



Câmara Municipal de Foz do Iguaçu

- 1.18. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão.
- 1.19. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
- 1.20. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
- 1.21. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
- 1.22. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
- 1.23. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
- 1.24. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
- 1.25. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
- 1.26. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
- 1.27. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
- 1.28. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
- 1.29. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
- 1.30. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
- 1.31. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
- 1.32. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
- 1.33. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante



Câmara Municipal de Foz do Iguaçu

um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

- 1.34. A solução proposta deve permitir ao administrador personalizar relatórios.
- 1.35. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
- 1.36. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
- 1.37. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
- 1.38. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
- 1.39. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.
- 1.40. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
- 1.41. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
- 1.42. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
- 1.43. A solução proposta deve suportar integração com solução APT.
 - 1.44. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
- 1.45. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
 - 1.45.1. Windows
 - 1.45.2. Linux
- 1.46. A solução proposta deverá suportar os seguintes servidores de banco de dados:
 - 1.46.1.1. Windows:
 - 1.46.1.2. Microsoft SQL Server
 - 1.46.1.3. Microsoft Banco de dados SQL do Azure
 - 1.46.1.4. MySQL Standard e Enterprise
 - 1.46.1.5. MariaDB
 - 1.46.1.6. PostgreSQL
 - 1.46.2. Linux:
 - 1.46.2.1. MySQL
 - 1.46.2.2. MariaDB
 - 1.46.2.3. PostgreSQL
- 1.47. A solução proposta deverá suportar as seguintes plataformas virtuais:
 - 1.47.1.1. Windows:
 - 1.47.1.2. VMware vSphere 6.7 e 7.0
 - 1.47.1.3. Estação de trabalho VMware 16 Pro
 - 1.47.1.4. Servidor Microsoft Hyper-V 2012 de 64 bits
 - 1.47.1.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits



Câmara Municipal de Foz do Iguaçu

- 1.47.1.6. Microsoft Servidor Hyper -V 2016 de 64 bits
- 1.47.1.7. Servidor Microsoft Hyper-V 2019 de 64 bits
- 1.47.1.8. Servidor Microsoft Hyper-V 2022 de 64 bits
- 1.47.1.9. Citrix XenServer 7.1 LTSR
- 1.47.1.10. Citrix XenServer 8.x
- 1.47.1.11. Oracle VM VirtualBox 6.x
- 1.47.2. Linux:
 - 1.47.2.1. VMware vSphere 6.7, 7.0 e 8.0
 - 1.47.2.2. VMware Desktop 16 Pro e 17 Pro
 - 1.47.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
 - 1.47.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
 - 1.47.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
 - 1.47.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
 - 1.47.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
 - 1.47.2.8. Citrix XenServer 7.1 e 8.x
 - 1.47.2.9. Oracle VM VirtualBox 6.x e7.x
- 1.48. A solução proposta deve suportar criptografia em vários níveis:
 - 1.48.1. Criptografia completa do disco – incluindo disco do sistema
 - 1.48.2. Criptografia de arquivos e pastas
 - 1.48.3. Criptografia de mídia removível
 - 1.48.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2
- 1.49. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
 - 1.49.1. A criptografia de arquivos em unidades de computador locais.
 - 1.49.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
 - 1.49.3. A criação de listas criptografadas de pastas em unidades de computador locais.
- 1.50. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
 - 1.50.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
 - 1.50.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
- 1.51. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
 - 1.51.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
 - 1.51.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
- 1.52. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia
- 1.53. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.



Câmara Municipal de Foz do Iguaçu

- 1.54. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.
- 1.55. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
- 1.56. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.
- 1.57. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.
- 1.58. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.
- 1.59. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.
- 1.60. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.
- 1.61. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.
- 1.62. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.
- 1.63. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.
- 1.64. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
- 1.65. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados, independentemente da localização e/ou usuário.
- 1.66. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
- 1.67. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
- 1.68. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
 - 1.68.1. Uso do Trusted Platform Module e configurações de senha.
 - 1.68.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.



Câmara Municipal de Foz do Iguaçu

- 1.69. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
- 1.70. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
- 1.71. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
 - 1.71.1. Instalação remota de software de terceiros
 - 1.71.2. Relatórios sobre software e hardware existentes
 - 1.71.3. Monitoramento para instalação de software não autorizado
 - 1.71.4. Remoção de software não autorizado
- 1.72. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
- 1.73. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
- 1.74. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
- 1.75. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
- 1.76. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.
- 1.77. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
- 1.78. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
- 1.79. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
- 1.80. A solução proposta deve permitir ao administrador aprovar atualizações.
- 1.81. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
- 1.82. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
- 1.83. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
- 1.84. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
- 1.85. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
- 1.86. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
- 1.87. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
- 1.88. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
- 1.89. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'.



Câmara Municipal de Foz do Iguaçu

- 1.90. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
- 1.91. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
- 1.92. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
- 1.93. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
- 1.94. A solução proposta deve apoiar a implantação do sistema operacional.
- 1.95. A solução proposta deve suportar Wake-on LAN e UEFI.
- 1.96. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
- 1.97. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
- 1.98. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
- 1.99. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
- 1.100. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.
- 1.101. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
- 1.102. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
- 1.103. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
- 1.104. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
- 1.105. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
 - 1.105.1. Inicie a instalação ao reiniciar ou desligar o computador.
 - 1.105.2. Instale o gerador necessário todos os pré-requisitos do sistema.
 - 1.105.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
 - 1.105.4. Baixe atualizações para o dispositivo sem instalá-las.
- 1.106. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
- 1.107. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
- 1.108. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
 - 1.108.1. CEF;



Câmara Municipal de Foz do Iguaçu

- 1.108.2. LEEF;
- 1.109. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
- 1.110. O relatório da solução proposta deve conter informações CVE.
- 1.111. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.3. Do módulo de gerenciamento simplificado

- 1.112. A solução proposta deve suportar arquitetura cloud;
- 1.113. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
- 1.114. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
- 1.115. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
- 1.116. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
- 1.117. A solução proposta deve atender as condições apontadas no item e subítemes 6.
- 1.118. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
- 1.119. A solução proposta deve incluir informações do endpoint:
 - 1.119.1. IP público de internet;
 - 1.119.2. IP interno do dispositivo;
 - 1.119.3. Versão do agente de proteção;
 - 1.119.4. Última comunicação com a console, contendo data e hora;
 - 1.119.5. Informações do sistema operacional;
- 1.120. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
- 1.121. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
- 1.122. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. Requisitos gerais

- 1.123. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
 - 1.123.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
- 1.124. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
- 1.125. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
- 1.126. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
- 1.127. A solução proposta deve suportar o subsistema Linux no Windows.
- 1.128. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
 - 1.128.1. Proteção contra ameaças sem arquivos (Fileless);
 - 1.128.2. Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;



Câmara Municipal de Foz do Iguaçu

- 1.129. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
- 1.130. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
- 1.131. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
- 1.132. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
- 1.133. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
- 1.134. A solução proposta deve fornecer análise comportamental baseada em machine learning.
- 1.135. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
- 1.136. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
 - 1.136.1. Controles de aplicativos,
 - 1.136.2. Controle web e dispositivos
 - 1.136.3. HIPS e Firewall
 - 1.136.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
 - 1.136.5. Gerenciamento de criptografia de arquivos e discos;
 - 1.136.6. Controle adaptativo para detecção de anomalias;
- 1.137. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
- 1.138. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
- 1.139. A solução proposta deve ter bancos de dados de reputação locais e globais.
- 1.140. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
- 1.141. A solução proposta deve incluir um módulo capaz, no mínimo, de:
 - 1.141.1. Bloqueio de aplicativos com base em sua categorização.
 - 1.141.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
 - 1.141.3. A adição de sub-redes e a modificação de permissões de atividade.
- 1.142. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
- 1.143. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
- 1.144. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem



Câmara Municipal de Foz do Iguaçu

ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

- 1.145. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
 - 1.145.1. Modo silencioso;
 - 1.145.2. Discos rígidos e dispositivos removíveis;
 - 1.145.3. De todos as contas de usuários do dispositivo.
- 1.146. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
 - 1.146.1. Exclusão imediata de dados;
 - 1.146.2. Exclusão de dados adiada.
- 1.147. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
 - 1.147.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
 - 1.147.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
- 1.148. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
- 1.149. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
- 1.150. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
- 1.151. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.
- 1.152. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
- 1.153. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
- 1.154. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
- 1.155. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
- 1.156. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
- 1.157. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
- 1.158. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
- 1.159. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.



Câmara Municipal de Foz do Iguaçu

- 1.182. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
- 1.183. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
- 1.184. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
- 1.185. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
 - 1.185.1. Filtro de anexos.
 - 1.185.2. Verificação de mensagens de email ao receber, ler e enviar.
- 1.186. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
- 1.187. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
- 1.188. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
- 1.189. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
- 1.190. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
- 1.191. A solução proposta deve incluir suporte ao protocolo IPv6.
- 1.192. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
- 1.193. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
- 1.194. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
- 1.195. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
- 1.196. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
- 1.197. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
- 1.198. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
- 1.199. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
- 1.200. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
- 1.201. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.



Câmara Municipal de Foz do Iguaçu

- 1.202. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
- 1.203. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
- 1.204. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
- 1.205. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
- 1.206. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
- 1.207. A solução proposta deve suportar endereços IPv6.
- 1.208. A solução proposta deve suportar verificação em duas etapas (autenticação).
- 1.209. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
- 1.210. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
- 1.211. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
- 1.212. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
- 1.213. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
- 1.214. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
- 1.215. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
- 1.216. A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos.
- 1.217. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
- 1.218. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi, Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hypervisor.
- 1.219. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
- 1.220. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
- 1.221. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
- 1.222. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.



Câmara Municipal de Foz do Iguaçu

- 1.223. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
- 1.224. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
- 1.225. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
- 1.226. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
- 1.227. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
- 1.228. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
- 1.229. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
- 1.230. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
- 1.231. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
- 1.232. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
- 1.233. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
 - 1.233.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
 - 1.233.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
- 1.234. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
- 1.235. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

4.5. Do módulo de gerenciamento de dispositivos móveis

- 1.236. O módulo deve ser integrado a console de gerenciamento;
- 1.237. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
 - 1.237.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)
- 1.238. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
 - 1.238.1. iOS 10–17 ou iPadOS 13–17
- 1.239. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
- 1.240. A solução proposta deve suportar dispositivos iOS supervisionados.
- 1.241. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.



Câmara Municipal de Foz do Iguaçu

- 1.242. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
- 1.243. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
- 1.244. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
- 1.245. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
- 1.246. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
- 1.247. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
- 1.248. A solução proposta deve ter recursos de containerização para dispositivos Android.
- 1.249. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
 - 1.249.1. Dados em contêineres
 - 1.249.2. Contas de e-mail corporativo
 - 1.249.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
 - 1.249.4. Nome do ponto de acesso (APN)
 - 1.249.5. Perfil do Android for Work
 - 1.249.6. Recipiente KNOX
 - 1.249.7. Chave do gerenciador de licença KNOX
- 1.250. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
 - 1.250.1. Todos os perfis de configuração instalados
 - 1.250.2. Todos os perfis de provisionamento
 - 1.250.3. O perfil iOS MDM
- 1.251. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
- 1.252. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .
- 1.253. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controle de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
 - 1.253.1. Critérios de verificação do dispositivo;
 - 1.253.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
- 1.254. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
- 1.255. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:



Câmara Municipal de Foz do Iguaçu

- 1.255.1. Cartões de memória e outras unidades removíveis
- 1.255.2. Câmera do dispositivo
- 1.255.3. Conexões Wi-Fi
- 1.255.4. Conexões Bluetooth
- 1.255.5. Porta de conexão infravermelha
- 1.255.6. Ativação do ponto de acesso Wi-Fi
- 1.255.7. Conexão de área de trabalho remota
- 1.255.8. Sincronização de área de trabalho
- 1.255.9. Definir configurações da caixa de correio do Exchange
- 1.255.10. Configurar caixa de e-mail em dispositivos iOS MDM
- 1.255.11. Configure contêineres Samsung KNOX.
- 1.255.12. Definir as configurações do perfil do Android for Work
- 1.255.13. Configurar e-mail/calendário/contatos
- 1.255.14. Defina as configurações de restrição de conteúdo de mídia.
- 1.255.15. Definir configurações de proxy no dispositivo móvel
- 1.255.16. Configurar certificados e SCEP
- 1.256. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
- 1.257. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
 - 1.257.1. Google Play, Huawei App Gallery e Apple App Store
 - 1.257.2. Portal de inscrição móvel KNOX
 - 1.257.3. Pacotes de instalação pré-configurados independentes
- 1.258. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
- 1.259. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
- 1.260. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
 - 1.260.1. VMware AirWatch 9.3 ou posterior
 - 1.260.2. MobileIron 10.0 ou posterior
 - 1.260.3. IBM MaaS360 10.68 ou posterior
 - 1.260.4. Microsoft Intune 1908 ou posterior
 - 1.260.5. SOTI MobiControl 14.1.4 (1693) ou posterior
- 1.261. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
- 1.262. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
 - 1.262.1. Google Play
 - 1.262.2. Galeria de aplicativos Huawei
 - 1.262.3. Loja de aplicativos da Apple
- 1.263. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
- 1.264. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.



Câmara Municipal de Foz do Iguaçu

- 1.265. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
- 1.266. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
- 1.267. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
- 1.268. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
- 1.269. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
- 1.270. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
- 1.271. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
- 1.272. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
- 1.273. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
- 1.274. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
- 1.275. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
- 1.276. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.6. Do módulo de EDR

- 4.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
- 4.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
- 4.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
- 4.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
- 4.6.5. Deve apresentar informações detalhadas contendo:
 - 4.6.5.1. Usuário que executou a ação;
 - 4.6.5.2. Informações acesso privilegiado;
- 4.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
- 4.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
- 4.6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado.



Câmara Municipal de Foz do Iguaçu

- (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)
- 4.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).
 - 4.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;
 - 4.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
 - 4.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.
 - 4.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
 - 4.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
 - 4.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
 - 4.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
 - 4.6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
 - 4.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
 - 4.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
 - 4.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
 - 4.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
 - 4.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
 - 4.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.
 - 4.6.24. Alterações no registro associadas à detecção.
 - 4.6.25. Histórico da presença de arquivos no dispositivo.
 - 4.6.26. Ações de resposta executadas pela aplicação.
 - 4.6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.
 - 4.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
 - 4.6.29. Processo
 - 4.6.30. Conexões de rede
 - 4.6.31. Alterações no registro
 - 4.6.32. Detalhes do download de objeto
 - 4.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).



Câmara Municipal de Foz do Iguaçu

- 4.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente
- 4.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
- 4.6.36. Impedir a execução de objetos
- 4.6.37. Isolamento de host
- 4.6.38. Excluir objeto do host ou grupo de hosts
- 4.6.39. Encerrar um processo no dispositivo
- 4.6.40. Colocar um objeto em quarentena
- 4.6.41. Execute a verificação do sistema
- 4.6.42. Execução remota de programa/processo/comando
- 4.6.43. Iniciar a varredura IoC para um grupo de hosts.

4.7. Requisitos para documentação da solução.

- 4.7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
- 4.7.2. Ajuda on-line para administradores
- 4.7.3. Ajuda on-line para melhores práticas de implementação
- 4.7.4. Ajuda on-line para proteção de servidores de administração
- 4.7.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
- 4.7.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

04. PRAZO DE GARANTIA

- a. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados na minuta do contrato.
- b. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

05. OBRIGAÇÕES DA CONTRATANTE

- a. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;
- b. Designar funcionário para acompanhar/fiscalizar a entrega;
- c. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;
- d. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;
- e. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;



Câmara Municipal de Foz do Iguaçu

- f. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis;

06. OBRIGAÇÕES DA CONTRATADA

- a. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;
- b. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;
- c. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- d. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

07. DA SUBCONTRATAÇÃO

- a. Não será admitida a subcontratação do objeto.

08. MODELO DE EXECUÇÃO DO OBJETO

Em até, 30 dias, a contar da assinatura do contrato, as novas licenças deverão ser fornecidas e registradas em nome de CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br , dentro da plataforma da desenvolvedora Kaspersky Global.

Quando que realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

09. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A execução do objeto seguirá a seguinte dinâmica:

- a. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.
- b. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.
- c. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.
- d. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica quando aplicável.
- e. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.
- f. Os prazos e critérios para recebimento e pagamento estão detalhados nos itens 7.3 a 7.4.
- g. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar

Assinado por 1 pessoa: PRESIDENTE DA CÂMARA MUNICIPAL DE FOZ DO IGUAÇU
Para verificar a validade das assinaturas, acesse <https://fozdoiguacu.1.doc.com.br/verificacao/ED06E-27445-F0009-960612-aritome@00jig1E8D8E2ZPA1-5-480886064>





Câmara Municipal de Foz do Iguaçu

execução do objeto do contrato através do termo de recebimento definitivo.

h. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

i. A apresentação da Nota Fiscal/fatura é indispensável a cada fornecimento de bem ou serviço, para fins de liquidação e pagamento da despesa, emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUAÇU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

j. Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

k. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

l. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

m. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

n. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 20 (vinte) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

o. Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

p. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a Contratada não regularize sua situação junto ao SICAF.



Câmara Municipal de Foz do Iguaçu

- q. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.
- r. Pagamento:
- i. Os pagamentos serão efetuados até o 10º (décimo) dia após o recebimento definitivo dos bens, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei nº 14.133/2021
- ii. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA/IBGE, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

Sanções:

- s. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:
- t. Dar causa à inexecução parcial do contrato;
- u. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- v. Dar causa à inexecução total do contrato;
- w. Deixar de entregar a documentação exigida para o certame;
- x. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- y. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- z. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
- aa. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;
- bb. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;
- cc. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- dd. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.
- ee. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;
- ff. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
- a) Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor,
- b) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver
- c) aplicado a sanção, pelo prazo máximo de 3 (três) anos.
- d) Direta, quando não se justificar a imposição de penalidade mais grave;
- e) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.9 a bem como nos demais casos que justifiquem a imposição da penalidade mais grave.
07. A fiscalização do contrato será realizada pelo servidor(a) designado:
08. A gestão do contrato será realizada pelo servidor (a) designado:



Câmara Municipal de Foz do Iguaçu

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

Tratamento diferenciado e favorecido a ser dispensado às microempresas, às empresas de pequeno porte e aos microempreendedores individuais conforme definido pelo documento de estudo técnico preliminar (ETP).

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As quantidades previstas a serem adquiridas, conforme os itens descritos, são:

Item	Descrição	SKU	Quantidade	Valor Unit.	Valor
<u>1</u>	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KAST J	160	R\$ 358,19	R\$ 57.310,40

A pesquisa de preço foi realizada considerando os parâmetros dispostos da Lei 14.133 no art. 23 § inciso IV – “*pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital*”. Do qual optou-se pelo menor preço ofertado.

Quanto à não utilização dos parâmetros dos § Incisos I e II do Art. 23, consultas no portal PNCF (Inciso I) e contratações similares feitas pela Administração Pública (II), conforme descrito no parágrafo anterior, torna-se ineficaz e escassa a busca por contratações similares em outros órgãos. Regendo-se pela economicidade, melhor tecnologia e melhores resultados pretendidos pelo órgão, consulta aos fornecedores torna-se mais eficaz.

12. ADEQUAÇÃO ORÇAMENTÁRIA

ITEM	DOTAÇÃO
------	---------

Assinado por [] pessoa. Para verificar a validade das assinaturas, acesse <https://fozdoiguacu.1.doc.com.br/verificacao/ED068-27445-80009-86005-810000-86005-4D>





Câmara Municipal de Foz do Iguaçu

1	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE
---	--





VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: 8D6E-2A15-90A9-AA4D

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

- ✓ WALDSON DE ALMEIDA DIAS (CPF 425.XXX.XXX-20) em 13/09/2024 11:04:35 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

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

<https://fozdoiguacu.1doc.com.br/verificacao/8D6E-2A15-90A9-AA4D>



ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em “adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos ocorridos no ano de 2018 (R\$ 11.635) e 2021 (R\$ 31.217,00 (Preço médio)) e já realizados, tendo em vista de que além da aquisição do sistema, foi também realizada no ano de 2023 (R\$ 6.980,00) a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, por medida de economicidade optou-se pela renovação com upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças de acordo com a

necessidade da CMFI , levando em consideração a ampliação do parque computacional que ocorreu nesses últimos anos e demandas futuras.

Notou-se ainda que a linha de produtos do desenvolvedor da solução passou por atualizações entregando novas versões de sua solução bem como mais recursos, a título de exemplo temos, portais de capacitação na solução, canais de suporte e a adoção da inteligência artificial para detecção e mitigação de vulnerabilidades.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
<u>1</u>	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R\$ 57.310,40

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.

A solução deve ter a capacidade de etiquetar/marcas computadores com base em Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.

A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.

A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:

Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB

- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:

Windows:

- VMware vSphere 6.7 e 7.0
- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, última comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:

Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

A solução deve ter capacidade de integração com a central de segurança do Windows Defender.

A solução deve suportar o subsistema Linux no Windows.

A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;
- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientais nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica, trata-se de um único item.

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações. Considerando que o mapa de gerenciamento de riscos tem natureza opcional, conforme previsto na NLL 14.133 e ato da presidência 133/2023.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;

- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;
- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/06/2024 às 09:38. Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que

há sério risco da licitação ser deserta. Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

Jeverson Siqueira
Cargo: Técnico de Informática
Matrícula: 202.045
Setor: Diretoria de Tecnologia



VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: AD30-E329-B4EC-1FF9

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

- ✓ JEVERSON SIQUEIRA (CPF 080.XXX.XXX-74) em 03/10/2024 08:41:08 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

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

<https://fozdoiguacu.1doc.com.br/verificacao/AD30-E329-B4EC-1FF9>





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

especificações técnicas mínimas do objeto, a fundamentação da contratação, a descrição da solução como um todo, as condições da garantia, os requisitos de habilitação, qualificação, técnica e capacidade operacional e de fornecimento, os requisitos da contratação, dentre outras informações, estão constantes em Termo de Referência, que é parte integrante deste Contrato independentemente de sua transcrição, ao qual também se declaram vinculados os contraentes.

3. CLÁUSULA TERCEIRA – DA LEGISLAÇÃO APLICÁVEL E DOS CASOS OMISSOS

3.1. Aplica-se a Lei n. 14.133/2021 à execução deste Contrato, sendo esta também a legislação a ser aplicadas aos casos omissos.

4. CLÁUSULA QUARTA – DO REGIME DE EXECUÇÃO

4.1. Os serviços serão executados sob o regime de execução indireta.

4.2. A execução dos serviços especificados neste Contrato e em Termo de Referência deverá ter início em até 30 dias, contados da assinatura do contrato, mediante fornecimento das licenças registradas em nome da CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ n. 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br, dentro da plataforma da desenvolvedora Karpersky Global.

4.2. Quando realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

4.3. Os serviços de instalação e manutenção deverão ser realizados na sede administrativa da CONTRATANTE, no endereço Travessa Oscar Muxfeldt, 81 - Centro, Foz do Iguaçu - PR, 85851-490

4.4. Os serviços a serem contratados constituem-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal da CONTRATANTE, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

4.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração, vedando-se qualquer relação entre elas que caracterize pessoalidade e subordinação direta.

4.6. Os serviços contratados são enquadrados como continuados, tendo em vista a sua necessidade permanente para a CONTRATANTE.

5. CLÁUSULA QUINTA – PREÇO

5.1. Em contra partida aos serviços prestados a CONTRATANTE pagará à CONTRATADA o valor mensal de até **R\$ XXXXX**, totalizando estimativa de pagamento anual de até **R\$ XXXXX**, conforme descrito na proposta apresentada pela empresa e constante no processo administrativo.

5.2. No valor indicado estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6. CLÁUSULA SEXTA – DO REAJUSTE





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

6.1. Mediante expresse pedido da CONTRATADA, os valores contratados poderão ser reajustados a cada 12 (doze) meses, contados a partir da data da proposta apresentada pela CONTRATADA, com aplicação do índice de variação do ICTI – Índice de Custo da Tecnologia da Informação, calculado pelo IPEA, para o mesmo período ou outro índice que o substitua.

6.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses para a próxima reajustamento, será contado a partir dos efeitos financeiros do último reajuste.

6.3. O reajuste previsto nesta cláusula poderá ser formalizado por Termo de Apostilamento.

7. CLÁUSULA SÉTIMA – DOS CRITÉRIOS DE MEDIÇÃO

7.1. Os Materiais entreguem dever estar em conformidade com as quantidades solicitadas dos itens já descritos neste documento;

7.2. A qualidade exigida dos equipamentos e materiais utilizados tem que estar de acordo com a qualidade de cada item, sendo vedada a utilização de materiais de qualidade inferior ou de não garantia.

7.3. Todos os pontos instalados devem ser certificados para assim constatar a qualidade do serviço e garantia de transmissão do mesmo.

7.4. Dos demais todos os itens devem ser novos seguidos rigidamente as especificações mínimas descritas na seção Requisitos da Contratação e amparados em seu prazo de garantia estabelecidos.

8. CLÁUSULA OITAVA – DO RECEBIMENTO

8.1. Os serviços serão recebidos provisoriamente no prazo de 05 (cinco) dias, para efeito de posterior verificação de sua conformidade com as especificações constantes na proposta;

8.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da CONTRATANTE, às suas custas, sem prejuízo da aplicação das penalidades;

8.3. Na impossibilidade de realização dos serviços, a empresa vencedora deverá substituir o serviço por outro com especificações iguais ou superiores;

8.4. Os serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação;

8.5. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;

8.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

9. CLÁUSULA NONA – DO PAGAMENTO

9.1. Os pagamentos serão efetuados até o 10º (décimo) dia após o recebimento definitivo dos produtos/serviços, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei nº 14.133/2021.

9.2. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

9.3. A apresentação da nota fiscal/fatura é indispensável a cada entrega de produtos ou prestação de serviços, para fins de liquidação e pagamento da despesa, a ser emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUAÇU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

9.4. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

9.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

9.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.7. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

9.8. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

9.9. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

9.11. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

10. CLÁUSULA DÉCIMA – DO PRAZO PARA RESPOSTA AOS PEDIDOS DE RE Pactuação DE PREÇOS E RESTABELECIMENTO DO EQUILÍBRIO ECONÔMICO

10.1. Quando for o caso de repactuação de preços e/ou de restabelecimento do equilíbrio econômico deste Contrato, será de 30 dias úteis o prazo resposta da CONTRATANTE, a contar da data de formalização do pedido por parte da CONTRATADA.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA INEXIGÊNCIA DE GARANTIAS À EXECUÇÃO DO CONTRATO

11.1. Dadas as características da contratação, não haverá exigência de garantia à execução do contrato.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

12. CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DOS PRODUTOS E SERVIÇOS

12.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados em termo de referência.

12.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

13. CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da Câmara Municipal, para o exercício de 2024 nas classificações: item 1 – 01.01.01.031.0001.2002.3.3.90.40.99.05 – AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE.

13.2. Nos exercícios seguintes, correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

14. CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DA CONTRATANTE

14.1. A CONTRATANTE obriga-se a:

14.1.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

14.1.2. Designar funcionário para acompanhar/fiscalizar a entrega;

14.1.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

14.1.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

14.1.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

14.1.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis.

15. CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

15.1. A CONTRATADA obriga-se a:

15.1.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

15.1.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

15.1.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

15.1.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

16. CLÁUSULA DÉCIMA SEXTA – DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

16.1.1. Dar causa à inexecução parcial do contrato;

16.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

16.1.3. Dar causa à inexecução total do contrato;

16.1.4. Deixar de entregar a documentação exigida para o certame;

16.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

16.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

16.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

16.1.9. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

16.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

16.1.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

16.1.12. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

16.1.13. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

16.1.13.1. Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor;

16.1.15. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, quando não se justificar a imposição de penalidade mais grave;

16.1.16. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 16.1.8 e bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

16.2. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor.

17. CLÁUSULA DÉCIMA SÉTIMA - DA OBRIGAÇÃO DE MANUTENÇÃO DAS CONDIÇÕES DE QUALIFICAÇÃO





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

17.1. A CONTRATADA obriga-se a manter, durante toda a execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições para a qualificação na contratação direta que precedeu a este instrumento;

18. CLÁUSULA DÉCIMA OITAVA - DA OBRIGAÇÃO DE RESERVA DE CARGOS PREVISTA EM LEI

18.1. A CONTRATADA, durante toda a execução do Contrato, obriga-se a cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

19. CLÁUSULA DÉCIMA NONA – MODELO DE GESTÃO DO CONTRATO

19.1. A execução do objeto seguirá a seguinte dinâmica:

19.1.1. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

19.1.2. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

19.1.3. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

19.1.4. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

19.1.5. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

19.1.6. Os prazos e critérios para recebimento e pagamento estão detalhados nas cláusulas 7 a 9 retro.

19.1.7. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

19.1.8. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

20. CLÁUSULA VIGÉSIMA – DA INEXECUÇÃO E DA EXTINÇÃO DO CONTRATO

20.1. A inexecução total ou parcial do contrato ensejará a sua extinção com as consequências contratuais e as previstas em lei, com fulcro no Título III, Capítulo VIII da Lei n. 14.133/2021, nos seguintes modos:

20.1.1. determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

20.1.2. consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

20.1.3. determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

20.2. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

20.2.1. não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

- 20.2.2. desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;
- 20.2.3. alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;
- 20.2.4. decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;
- 20.2.5. caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;
- 20.2.6. atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto;
- 20.2.7. atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas;
- 20.2.8. razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade CONTRATANTE.
- 20.3. O descumprimento, por parte da CONTRATADA, de suas obrigações legais e/ou contratuais assegurará ao CONTRATANTE o direito de extinguir o contrato a qualquer tempo, independentemente de aviso, interpelação judicial e/ou extrajudicial.
- 20.4. A extinção por ato unilateral do CONTRATANTE sujeitará a CONTRATADA à multa rescisória de até 10% (dez por cento) sobre o valor do saldo do contrato existente na data da extinção, independentemente de outras penalidades.
- 20.5. Caso o valor do prejuízo do CONTRATANTE advindo da extinção contratual por culpa da CONTRATADA exceder o valor da Cláusula Penal prevista no parágrafo anterior, esta valerá como mínimo de indenização, na forma do disposto no art. 416, parágrafo único, do Código Civil.
- 20.6. A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.
- 20.7. A CONTRATANTE poderá rescindir o presente instrumento contratual, sem qualquer ônus à Administração, quando da conclusão de eventual novo procedimento de contratação de interesse público para objeto afim.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – DA VIGÊNCIA

- 21.1. O presente Contrato terá validade de 36 (trinta e seis) meses, contados da data da assinatura, podendo ser prorrogado, a critério da Administração, conforme o disposto no art. 107, da Lei n. 14.133/2021 e suas alterações posteriores.
- 21.2. A prorrogação deste contrato deverá ser promovida mediante celebração de termo aditivo.

22. CLÁUSULA VIGÉSIMA SEGUNDA – DA FISCALIZAÇÃO

- 22.1. O acompanhamento e a fiscalização da execução das obrigações oriundas deste contrato ficarão a cargo do Gestor José Marceo Nicoletti Teixeira, e do Fiscal de Contratos, Jeverson Siqueira, e consiste na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

representantes da CONTRATANTE, especialmente designados, na forma do art. 117 da Lei nº 14.133/2021.

22.2. O fiscal do contrato deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 117 da Lei nº 14.133/2021.

22.3. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Contrato e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 156 e 137 da Lei nº 14.133/2021.

22.4. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade com art. 120 da Lei nº 14.133/2021.

23. CLÁUSULA VIGÉSIMA TERCEIRA – DA SUBCONTRATAÇÃO

23.1. É vedada a subcontratação total ou parcial do objeto deste Termo de Contrato.

24. CLÁUSULA VIGÉSIMA QUARTA – DAS VEDAÇÕES

24.1. É vedado à CONTRATADA:

24.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

24.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

25. CLÁUSULA VIGÉSIMA QUINTA – DAS ALTERAÇÕES

25.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos art. 124 a 136 da Lei n. 14.133/2021.

26. CLÁUSULA VIGÉSIMA SEXTA – DA PUBLICAÇÃO

26.1. A CONTRATANTE providenciará a publicação deste contrato no Diário Oficial do Município de Foz do Iguaçu, na página da Câmara Municipal de Foz do Iguaçu nos termos do art. 174 da Lei n. 14.133/2021 e no Portal Nacional de Contratações Públicas (PNCP), para fins de garantia a ampla publicidade.

27. CLÁUSULA VIGÉSIMA SÉTIMA – DO FORO

27.1. Fica eleito o foro desta cidade de Foz do Iguaçu, Estado do Paraná, para dirimir toda e qualquer questão que derivar deste contrato.

E por estarem justas e acordadas, assinam as partes o presente instrumento, na presença de duas testemunhas, que também o subscrevem, para que surtam todos os efeitos jurídicos e legais.





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

Foz do Iguaçu, xx de xxxxx de 2024.

**CÂMARA MUNICIPAL DE FOZ DO
IGUAÇU**

João José Arce Morales

XXXXXXXXXXXX
XXXXXXXXXXXX

Testemunhas:

Nome: XXXXXX

RG: XXXXXX

CPF: XXXXXXXX

Nome: XXXXXXXXXXX

RG: XXXXXXXX

CPF XXXXXXXX





Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

ANEXO IV - MODELO DE PROPOSTA DE PREÇOS PREGÃO, NA FORMA ELETRÔNICA, Nº 06/2024

REF: PREGÃO, NA FORMA ELETRÔNICA, Nº 06/2024-TIPO MENOR PREÇO

A empresa _____, estabelecida na _____, no bairro _____, no Município de _____, no Estado de _____, no n.º _____, na Prefeitura sob o n.º _____ e no Estado sob o n.º _____, CNPJ n.º _____, telefone n.º (____) _____ e e-mail _____, pela presente e consoante as especificações técnicas contidas no Edital, vem propor os valores abaixo para fornecimento de licenças antivírus do Pregão, na forma Eletrônica, nº 06/2024, conforme segue:

ITEM	DESCRIÇÃO	SKU	QNT	VALOR UNITÁRIO	VALOR TOTAL
1	Licença Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal license	KL4066KASTJ	160		

O **PREÇO TOTAL** apresentado na presente proposta é de R\$ _____ (valor por extenso).

Nesta proposta de percentual de desconto e preço estão considerados obrigatoriamente:

- O atendimento às especificações detalhadas do objeto, consoante Anexo I deste Edital;
- A inclusão de todas as despesas que influenciam nos custos, tais como despesas com custo, transporte e frete, tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), obrigações sociais, trabalhistas, fiscais, encargos comerciais ou de qualquer natureza e todos os ônus diretos e indiretos,
- O prazo de validade da proposta é de 90 (noventa) dias, a contar da data da sessão do pregão, na forma eletrônica.

Esta empresa declara que está ciente e cumprirá, integralmente, todas as cláusulas do EDITAL retro citado.

Foz do Iguaçu, _____ de _____ de _____.

Assinatura do representante legal da empresa proponente
NOME:
RG:
CARGO:





VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: E719-274A-F498-8605

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

- ✓ PRESIDENTE DA CÂMARA MUNICIPAL DE FOZ DO IGUAÇU (CPF 029.XXX.XXX-16) em 24/10/2024
10:44:13 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

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

<https://fozdoiguacu.1doc.com.br/verificacao/E719-274A-F498-8605>