Prefetura Municipal de Pedro Leopoldo
Dr. Cristiano Otoni, 555 - Centro
33250-006 - Pedro Leopoldo/MG

SETOR DE LICITAÇÕES
Fone: (31) 3660-5155
E-mail:licitacao@pedroleopoldo.mg.gov.br

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

EDITAL DE PREGÃO ELETRÔNICO

Processo Licitatório:	032/2024
Modalidade:	PREGÃO ELETRONICO
Número da Licitação:	027/2024
Aquisição de:	Serviços
Tipo de licitação:	Menor preço por lote

1. PREÂMBULO

O **MUNICÍPIO DE PEDRO LEOPOLDO,** com endereço na Rua Dr. Cristiano Otoni nº 555, Centro, na cidade de Pedro Leopoldo, Minas Gerais, CEP: 33250-006, torna público a abertura do **Processo Licitatório nº 032/2024 - Modalidade: Pregão Eletrônico nº 027/2024, Contratação de Serviço** especificados abaixo, pelo critério de julgamento **Menor preço por Lote** sob a regência da Lei Federal nº 14.133/2021; do Decreto Federal nº 10.024/2019; do Decreto Federal nº 11.871/2023; do Decreto Municipal nº 2.219 de 10/04/2023 e da Lei Complementar nº 123/2006, alterada pela Lei Complementar nº 147/2014, e demais normas complementares aplicáveis e condições fixadas neste Edital e seus Anexos.

Contato através do telefone (31) 3660-5114, e-mail: licitacao@pedroleopoldo.mg.gov.br e site http://www.pedroleopoldo.mg.gov.br.

RECEBIMENTO DAS PROPOSTAS: início às 18h do dia 20/12/2024 até às 13h30min do dia 17/01/2025

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: Às 13h30min do dia 17/01/2025

REFERÊNCIA DE TEMPO: Horário de Brasília (DF).

ENDEREÇO ELETRÔNICO: http://www.licitardigital.com.br

1.1. **DISPOSIÇÕES PRELIMINARES:**

1.1.1. O fornecedor deverá observar as datas e os horários limites previstos para a abertura das propostas, atentando também para a data e horário para início da disputa.

1.1.2. Os trabalhos serão realizados em sessão pública através do site Licitar Digital pelo(a) **PREGOEIRO (A)** e **EQUIPE DE APOIO**, designados pela **Portaria nº 15.834/2024**, contida nos autos do processo.

1.1.3. O Edital e seus Anexos poderão ser obtidos gratuitamente no site a Prefeitura Municipal de Pedro Leopoldo, através do endereço eletrônico www.pedroleopoldo.mg.gov.br e também na Plataforma de Licitações Licitar Digital, através do endereço eletrônico www.licitardigital.com.br.

1.1.4. Toda e qualquer alteração que possivelmente ocorrer neste Edital, tais como errata, adendo, suspensão ou revogação, deverá ser consultada pelos pretensos licitantes no endereço eletrônico www.licitardigital.com.br, bem como, no site da Prefeitura Municipal de Pedro Leopoldo, www.pedrolepoldo.mg.gov.br.

1.1.5. A Administração não se responsabilizará caso o pretenso licitante não acesse o e-mail informado ou não visualize a alteração no site supracitado, consequentemente desconhecendo o teor dos Avisos publicados.

1.1.6. As dúvidas pertinentes a presente licitação serão esclarecidas pela Gerência de Compras e Licitações do Município de Pedro Leopoldo no seguinte endereço e contatos:

Endereço: Rua Dr. Cristiano Otoni nº 555 Centro, Pedro Leopoldo/MG CEP 33250-006;
Telefone: (31) 3660-5114;
E-mail: licitacao@pedroleopoldo.mg.go.br;
Horário de atendimento: de segunda a sexta-feira das 12h às 17h.

1.1.7. Integram o presente edital, os seguintes anexos:

I - Termo de Referência;
II - Minuta do Contrato.

2. DO OBJETO

2.1**.** O presente Edital tem por objetivo receber propostas para o **PREGÃO ELETRÔNICO**, Tipo **MENOR PREÇO POR LOTE**, **Contratação de empresa especializada para prestação de serviços de segurança de rede de computadores composta por firewall com funcionalidades UTM (Unified Threat Management) incluindo serviços de suporte especializado, para atender as demandas da Secretaria de Administração, de acordo com o Edital e seus anexos.**

2.2. O fornecimento será de acordo com Termo de Referência (Anexo I do Edital), solicitação e autorização da Secretaria.

2.3. Os procedimentos para acesso ao Pregão Eletrônico estão disponíveis no site Licitar Digital no endereço eletrônico: www.licitardigital.com.br.

2.4. Conforme o Decreto 10.024/2019 no Art. 26: Após a divulgação do edital no sítio eletrônico, os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço,até a data e o horário estabelecidos para abertura da sessão pública.

2.5. Os documentos relativos à habilitação, solicitados no item 09 do presente edital, deverão ser ANEXADOS, OBRIGATORIAMENTE, juntamente com a proposta na página da Licitar Digital, em local próprio para documentos, antes da abertura da Sessão Pública.

2.5.1 OS LICITANTES QUE NÃO ANEXAREM A DOCUMENTAÇÃO NA PLATAFORMA, SERÃO CONSIDERADAS INABILITADAS.

OBS. ESSES DOCUMENTOS SÓ ESTARÃO DISPONÍVEIS APÓS O ENCERRAMENTO DA DISPUTA DO PREGÃO.

3. DAS CONDIÇÕES PARA PARTICIPAÇÃO

3.1. Poderão participar deste Pregão Eletrônico as Pessoas Físicas e Jurídicas, que atenderem a todas as exigências quanto à documentação constantes neste Edital e pessoas legalmente constituídas.

3.2. Os interessados deverão estar previamente cadastrados na plataforma de licitações, Licitar Digital: www.licitardigital.com.br.

3.3. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico.

3.3.1. O acesso do operador ao pregão, para efeito de encaminhamento de proposta de preço e lances sucessivos de preços, em nome do licitante, somente se dará mediante prévia definição de senha privativa.

3.3.2. A chave de identificação e a senha dos operadores poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado ou por iniciativa da Licitar Digital.

3.3.3. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao Município de Pedro Leopoldo e ao provedor do sistema Licitar Digital a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.3.4. O credenciamento do prestador de serviços e de seu representante legal junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico.

3.3.5. Caberá ao prestador de serviços acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou da desconexão do seu representante.

3.4. Conforme previsão do art. 4º do Decreto Municipal 2.295 de 23 de Abril de 2024 que regulamenta o disposto nos Artigos 42 a 45 e 47 a 49 da Lei Complementar 123/2006, terão tratamento favorecido, diferenciado e simplificado, as Microempresas ou equiparadas **sediadas no Município de Pedro Leopoldo**, nos seguintes casos:

3.4.1. Quando houver a participação de no mínimo 03 (três) empresas, **sediadas no município**, potenciais fornecedoras, que estejam devidamente cadastradas no segmento e ramo de interesse do Poder Executivo, e que possam cumprir as exigências previstas no instrumento convocatório, será aplicado a prioridade por Microempreendedor Individual, Microempresa e Empresa de Pequeno Porte, até o limite de 10% (dez por cento) do melhor preço válido, conforme §3º do Art. 48 da Lei Complementar Federal nº 123/2006.

3.4.2. O Poder Executivo disponibilizará em seu sítio eletrônico o link para cadastramento das potenciais empresas locais de forma a facilitar o acesso as compras públicas municipais, bem como a divulgação atualizada das empresas cadastradas, para fins de publicidade.

3.5. Os proponentes assumem todos os custos de preparação e apresentação de suas propostas e o **Município de Pedro Leopoldo** não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório;

3.6. Não será admitida nesta licitação a participação de empresas:

3.6.1. Empresas que estejam sob processo de falência.

3.6.2. Empresas/Pessoa Física que tenham sido declaradas inidôneas para licitar e contratar com a Administração Pública.

3.6.3. Empresas/Pessoa Física que estejam suspensas ou impedidas de licitar e contratar com a Administração Pública deste Município, durante o prazo da sanção aplicada.

3.6.4. Empresas/Pessoa Física que se enquadrem nas vedações de participação previstas no art. 14 da Lei nº 14.133/2021:

3.6.4.1. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta, estendendo-se a vedação 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 comprovado o ilícito ou utilização fraudulenta da personalidade jurídica do licitante;

3.6.4.2. 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, devendo essa proibição constar expressamente do edital de licitação;

3.6.4.3. 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.

3.6.5. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público de órgão ou entidade licitante ou 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 previsto no art. 9º, §1º da Lei Federal nº 14.133/2021.

3.6.5.1. As vedações estendem-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, conforme previsto no art. 9º, §2º, da Lei Federal nº 14.133/2021.

3.6.6. Sociedade estrangeira não autorizada a funcionar no País.

3.7. O licitante que cumprir os requisitos legais para qualificação como Microempresa (ME) ou equiparadas, nos termos do art. 3º da Lei Complementar n º 123/2006, que não estiver sujeito a quaisquer dos impedimentos do §4º deste artigo, caso tenha interesse em usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 da lei citada, deverá comprovar sua condição de ME, EPP, ou Equiparadas através de Declaração, em campo próprio do sistema, de acordo com o item 4.7.

3.8. O licitante que apresentar declaração falsa responderá por seus atos civil, penal e administrativamente.

4. DO CREDENCIAMENTO NO SISTEMA E DA EFETIVA PARTICIPAÇÃO

4.1. O Pregão Eletrônico será realizado em sessão pública, por meio da internet, mediante condições de segurança (criptografia e autenticação) em todas as suas fases.

4.2. Para acesso ao sistema eletrônico, os interessados na participação do Pregão Eletrônico deverão dispor de chave de identificação e senha pessoal (intransferíveis), obtidas através do site da Plataforma de Licitações da Licitar Digital (www.licitardigital.com.br).

4.3. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como, seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao Município de Pedro Leopoldo, ao provedor do sistema ou ao órgão promotor da licitação, a responsabilidade por eventuais danos decorrentes do uso indevido do acesso.

4.4. O credenciamento do licitante e de seu representante legal junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para a realização das transações inerentes ao pregão eletrônico.

4.5. A participação no Pregão Eletrônico se dará por meio da digitação da senha pessoal do credenciado e subsequente encaminhamento da proposta de preços e documentos de habilitação, exclusivamente por meio do sistema eletrônico, observando data e horário limite estabelecido.

4.6. O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas neste Edital.

4.7. COMO CONDIÇÃO PARA PARTICIPAÇÃO NO PREGÃO, A LICITANTE ASSINALARÁ "SIM" OU "NÃO" EM CAMPO PRÓPRIO DO SISTEMA ELETRÔNICO, RELATIVO ÀS SEGUINTES DECLARAÇÕES:

( ) Declaro que não incorro nas condições impeditivas do art. 14 da Lei Federal nº 14.133/21.

( ) Declaro que atendo aos requisitos de habilitação, conforme disposto no art. 63, inciso I, da Lei Federal nº 14.133/21.

( ) Declaro que cumpro as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, conforme art. 63, inciso IV, da Lei Federal nº 14.133/21.

( ) Declaro que a proposta apresentada para essa licitação está em conformidade com as exigências do instrumento convocatório e me responsabilizo pela veracidade e autenticidade dos documentos apresentados.

( ) Declaro que minha proposta econômica 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 da proposta, conforme art. 63, §1º, da Lei Federal nº 14.133/21.

( ) Declaro que estou ciente do edital e concordo com as condições locais para o cumprimento das obrigações objeto da licitação, conforme o art. 67, inciso VI, da Lei Federal nº 14.133/21;

( ) Declaro para fins do disposto no inciso VI do art. 68, da Lei nº 14.133/21, que não emprego menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprego menor de 16 (dezesseis) anos, salvo menor, a partir dos 14 (quatorze) anos, na condição de aprendiz, nos termos do inciso XXXIII, do art. 7º, da Constituição Federal/88.

( ) Declaro que não possuo, em minha cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal/88.

( ) Declaro para os devidos fins legais, sem prejuízo das sanções e multas previstas neste ato convocatório, estar enquadrado como ME/EPP/Cooperativa, conforme a Lei Complementar nº 123/2006, cujos termos declaro conhecer na íntegra, estando apto, portanto, a exercer o direito de preferência, observado também o disposto nos §§ 1º ao 3º do artigo 4º da Lei Federal n. 14.133/2021.

( ) Sim, ME ( ) Sim, EPP ( ) Não, outros enquadramentos.

4.8. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5. DO(S) PEDIDO(S) DE ESCLARECIMENTO

5.1. Os interessados poderão solicitar esclarecimentos e informações, **em até 03 (três) dias úteis** antes da data fixada para realização da sessão pública do pregão, devendo protocolar o pedido diretamente no site www.licitardigital.com.br, no local específico dentro do processo licitatório em análise.

5.1.1. Os esclarecimentos e as informações serão prestados no prazo de **03 (três) dias úteis**, limitado ao último dia útil anterior à data de abertura do certame.

5.2. A resposta do(a) Pregoeiro(a) ao **pedido de esclarecimento** formulado será divulgada no site www.licitardigital.com.br, em campo específico, **ficando os interessadas em participar do certame, obrigadas a acessá-la para a obtenção das informações prestadas.**

6. DA IMPUGNAÇÃO AO EDITAL

6.1. Até **03 (três) dias úteis** antes da data fixada para abertura do certame, qualquer pessoa poderá impugnar o Ato Convocatório deste Pregão, devendo encaminhar o pedido diretamente pelo site www.licitardigital.com.br, no local específico dentro do processo licitatório em análise.

6.1.1. Caberá ao agente de contratação se manifestar, motivadamente, a respeito da(s) impugnação(ões), proferindo sua decisão no prazo de 03 (três) dias úteis, contados da data de recebimento, limitado ao último dia útil anterior à data da abertura do certame.

6.1.2. A decisão sobre a impugnação será publicada em campo específico na plataforma Licitar Digital.
6.2. Caso seja acolhida a impugnação contra o Ato Convocatório, será designada nova data para realização do Certame.

6.3. Não serão conhecidas as impugnações e os recursos apresentados fora do prazo legal e/ou subscritos por representante não habilitado legalmente ou não identificado no processo para responder pelo proponente.

7. DA PROPOSTA ELETRÔNICA

7.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

7.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha intransferíveis.

7.3. No preenchimento da proposta eletrônica deverão, obrigatoriamente, ser informadas no campo próprio as ESPECIFICAÇÕES e MARCAS dos produtos ofertados, quando for o caso, conforme a ficha técnica descritiva do produto. A não inserção de arquivos ou informações contendo as especificações e marcas dos produtos neste campo, implicará a desclassificação da empresa/pessoa física, face à ausência de informação suficiente para classificação da proposta. O OBJETO deverá estar totalmente dentro das especificações contidas no Termo de Referência.

7.4. Nos preços cotados deverão estar inclusos todos os custos e demais despesas e encargos inerentes ao produto até sua entrega no local fixado por este edital.

7.5. O encaminhamento de proposta para o sistema eletrônico pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances, bem como quaisquer ônus decorrentes da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

7.6. A validade da proposta será de 60(sessenta) dias, contados a partir da data da sessão pública do Pregão.

7.7. Na hipótese de o licitante ser ME/EPP será necessário a informação desse regime fiscal no campo próprio sob pena do licitante enquadrado nesta situação não utilizar dos benefícios do direito de preferência para o desempate, conforme estabelece a Lei Complementar 123/2006.

7.8. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

7.9. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

7.10. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do(a) Pregoeiro(a) e para acesso público após o encerramento do envio de lances.

7.11. Os documentos complementares à proposta e à habilitação, quando necessários à confirmação daqueles exigidos no edital e já apresentados, se houver, serão encaminhados pelo licitante melhor classificado após o encerramento do

envio de lances no prazo definido pelo(a) pregoeiro(a), de no **mínimo 02 (duas) horas**, sob pena de inabilitação, podendo ser prorrogado.

7.12. 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.

7.12.1. Nestes casos, a licitante deverá encaminhar a documentação original ou a cópia autenticada exigida, no **prazo máximo de 03 (três) dias úteis**, contados da data da solicitação do(a) pregoeiro(a), via sistema.

7.13. Havendo necessidade de analisar minuciosamente os documentos exigidos, o(a) Pregoeiro(a) suspenderá a sessão, informando no "*chat*" a nova data e horário para a continuidade da mesma.

7.14. Serão desclassificadas as propostas que conflitem com as normas deste edital ou da Legislação em vigor.

7.15. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

7.16. O lance deverá ser ofertado em conformidade com o objeto do edital, se for global, preço total, se for unitário, pelo valor unitário para os itens. Deve-se observar um valor de diferença mínima entre os lances, assim evitando valores irrisórios quando o valor do objeto for de grande porte.

7.17. Atendidos todos os requisitos, será considerada vencedora a licitante que oferecer o MENOR PREÇO.

8. DOS LANCES E ACEITABILIDADE DA PROPOSTA VENCEDORA

8.1. Aberta a etapa competitiva, os representantes dos fornecedor(es) deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

8.2. Só serão aceitos lances cujos valores forem inferiores ao último lance que tenha sido anteriormente registrado no sistema.

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

8.4. As propostas não deverão estar com valores superiores ao máximo fixado no Edital (REFERENTE AO VALOR UNITÁRIO) e não havendo lances com valores iguais ou inferiores, serão desclassificados.

8.5. Fica a critério do(a) Pregoeiro(a) a autorização da correção de lances com valores digitados errados ou situação semelhante, mesmo que, antes do início da disputa de lances;

8.6. Durante o transcurso da sessão pública os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais participantes.

8.7. Caso não sejam apresentados lances, será verificada a conformidade entre a proposta de menor preço e valor estimado para a contratação.

8.8. Na hipótese de o sistema eletrônico desconectar para o(a) Pregoeiro(a) no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

8.9. Quando da desconexão do sistema eletrônico para o(a) pregoeiro(a) persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente decorridas vinte e quatro horas após a comunicação do fato aos participantes, no sítio eletrônico utilizado para divulgação.

8.10. O tipo de julgamento será no modo de disputa **aberto**, de que trata o inciso I do caput do art. 31 do Decreto nº 10.024/2019, a etapa de envio de lances na sessão pública durará dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

8.11. A prorrogação automática da etapa de envio de lances, de que trata o caput, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.

8.12. Na hipótese de não haver novos lances na forma estabelecida no caput e no §1º do art. 32 do Decreto 10.024/19, a sessão pública será encerrada automaticamente.

8.13. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, o sistema identificará 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 artigos 44 e 45 da LC nº 123, de 2006.

8.13.1. 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.

8.13.2. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 3 (três) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

8.13.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresas e empresas 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.

8.13.4. 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.

8.13.5. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que 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.

8.13.6. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60, da Lei nº 14.133/2021, assegurando-se a preferência, sucessivamente, aos bens:

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

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

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

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

8.13.6.5. Empresas brasileiras;

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

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

8.13.7. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

8.14. Encerrada a sessão pública sem prorrogação automática pelo sistema, o(a) pregoeiro(a) poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço disposto no parágrafo único do art. 7º do Decreto 10.024/2019, mediante justificativa.

8.15. Face à imprevisão do tempo extra, os participantes deverão estimar o seu valor mínimo de lance a ser ofertado, evitando assim, cálculos de última hora, que poderá resultar em uma disputa frustrada por falta de tempo hábil.

8.16. Facultativamente, o(a) Pregoeiro(a) poderá encerrar a sessão pública mediante encaminhamento de aviso de fechamento iminente dos lances e subsequente transcurso do prazo de trinta minutos, findo o qual será encerrada a recepção de lances. Neste caso, antes de anunciar o vencedor, o(a) Pregoeiro(a) poderá encaminhar, pelo sistema eletrônico contraproposta diretamente ao proponente que tenha apresentado o lance de menor preço, para que seja obtido preço melhor, bem como decidir sobre sua aceitação.

8.17. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances ou, quando for o caso, após negociação e decisão pelo(a) pregoeiro(a)acerca da aceitação do lance de menor valor.

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

8.19. Quando houver apenas um item por lote, o sistema ao final da sessão de disputa automaticamente atualizará a proposta do licitante pelo melhor lance ofertado. No caso de haver mais de um item por lote, o sistema fará a divisão dos valores entre os itens de forma proporcional. Excepcionalmente, o(a) Pregoeiro(a) poderá liberar a atualização de proposta manual diretamente na plataforma para que o licitante faça o preenchimento do(s) valor(es) do(s) item(s) do(s) lote(s) livremente, caso entenda necessário.

8.19.1. Caso seja necessário a comprovação da exequibilidade dos valores apresentados, o(a) Pregoeiro(a) poderá solicitar que, no **prazo de 02 (duas) horas**, o licitante envie, através do sistema, documentos complementares, tais como: notas fiscais, planilhas, contratos ou instrumentos equivalentes.

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

8.21. O(a) Pregoeiro(a) poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no **prazo de 02 (duas) horas**, sob pena de não aceitação da proposta.

8.22. O prazo estabelecido poderá ser prorrogado pelo(a) Pregoeiro(a) por solicitação escrita e justificada do licitante, formulada antes de findo o prazo, e formalmente aceita pelo(a) Pregoeiro(a).

8.23. Dentre os documentos passíveis de solicitação pelo(a) Pregoeiro(a), destacam-se os que contenham as características do produto ofertado, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo(a) Pregoeiro(a), sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

8.24. Se a proposta ou lance de menor valor não for aceitável, ou se o licitante desatender às exigências habilitatórias, o(a) Pregoeiro(a) examinará a proposta ou lance subsequente, verificando a sua compatibilidade e a habilitação do participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o Edital. Também nessa etapa o(a) Pregoeiro(a) poderá negociar com o participante para que seja obtido preço melhor.

8.24.1. Se tratando de Lote, a desclassificação de um único item do lote implicará a desclassificação da proposta para todo o lote, ou seja, a proposta somente será aceita se atender aos requisitos para todos os itens que compõem o lote.

8.25. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes pelo "***chat***".
8.26. Havendo necessidade, o(a) Pregoeiro(a) suspenderá a sessão, informando no **"*chat*"** a nova data e horário para a sua continuidade.
8.27. Constatando o atendimento das exigências fixadas no Edital e inexistindo interposição de recursos, o objeto será adjudicado ao autor da proposta ou lance de menor preço.

9. DA HABILITAÇÃO

9.1. HABILITAÇÃO JURÍDICA:

9.1.1. Ato constitutivo, estatuto ou contrato social e suas alterações ou instrumento consolidado, devidamente registrado na junta Comercial em se tratando de sociedades empresárias ou cooperativas, e, no caso de sociedade de ações, acompanhado de documentos de eleição ou designação de seus administradores;

9.1.2. Ato Constitutivo devidamente registrado no Registro Civil de Pessoas Jurídicas tratando-se de sociedade não empresária, acompanhado de prova da diretoria em exercício;

9.1.3. Registro empresarial na Junta Comercial, no caso de empresa individual;

9.1.4. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no país.

9.1.5. Apresentar Alvará de Funcionamento, exceto para MEI (Microempreendedor Individual) ou nos casos que a lei dispensar.

9.1.5.1. Fica condicionado ao licitante apresentar a devida documentação de dispensa do Alvará de Funcionamento, sob pena de inabilitação.

9.1.6. Se a documentação de habilitação **não estiver completa** e correta ou contrariar qualquer dispositivo deste Edital e seus anexos, **o licitante será inabilitado**.

9.1.7. Uma vez incluído no processo, nenhum documento será devolvido, exceto os originais, se substituídos por cópias autenticadas.

9.2. REGULARIDADE FISCAL:

9.2.1. Prova de inscrição no CNPJ - Cadastro Nacional de Pessoas Jurídicas (expedida pela Secretaria da Receita Federal).

9.2.2. Prova de Regularidade Relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND **Conjunta** de Tributos Federais e Relativos ao INSS, de acordo com Portaria da Procuradoria Geral da Fazenda Nacional / Receita Federal do Brasil nº 1751, de 02 de outubro de 2014).

9.2.3. Prova de Regularidade relativa ao **FGTS** - Fundo de Garantia por Tempo de Serviço (emitida pela Caixa Econômica Federal).

9.2.4. Prova de Regularidade Relativa à Fazenda Estadual (expedida pela Secretaria Estadual de Fazenda/Administração).
9.2.5. Prova de Regularidade Relativa à Fazenda Municipal (expedida pela Secretaria Municipal de Fazenda/Administração).

9.3. REGULARIDADE TRABALHISTA

9.3.1. Certidão Negativa de Débitos Trabalhistas – **CNDT** - (Lei Federal n.º12.440/2011 – DOU 1 de 08.07.2011).

9.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

9.4.1. Certidão negativa de falência e concordata ou Certidão cível negativa, expedida pelo(s) cartório(s) distribuidor(es) da sede da pessoa jurídica - não constando no documento o prazo de validade, este será de **90 (Noventa) dias.**

9.5. QUALIFICAÇÃO TÉCNICA

9.5.1. Apresentar Atestado (s) de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a licitante realizado ou estar realizando fornecimento pertinente e compatível com o objeto a ser contratado, de forma satisfatória;

9.5.2. Demais documentos que compõem o rol da Lei Geral de Licitações para a modalidade de aquisição pretendida.

9.6. DISPOSIÇÕES GERAIS DA HABILITAÇÃO

9.6.1. O(a) Pregoeiro(a) considerará o proponente inabilitado caso a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus Anexos.

9.6.2. Documentos apresentados com a validade expirada acarretarão na inabilitação do proponente.

9.6.3. O(a) Pregoeiro(a) reserva-se o direito de solicitar das licitantes, em qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre documentos já entregues, fixando-lhes prazo para atendimento;

9.6.4 A falta de quaisquer dos documentos exigidos no Edital implicará inabilitação da licitante, sendo vedada, sob qualquer pretexto, a concessão de prazo para complementação da documentação exigida para a habilitação.

9.6.5. Os documentos de habilitação deverão estar em nome da licitante, com o número do CNPJ e respectivo endereço referindo-se ao local da sede da empresa licitante. Não se aceitará, portanto, que alguns documentos se refiram à matriz e outros á filial. Caso o licitante seja a Matriz e a executora do fornecimento seja a filial, os documentos referentes à habilitação deverão ser apresentados em nome de ambas, simultaneamente.

9.6.6. Os documentos de habilitação deverão estar em plena vigência e, na hipótese de inexistência de prazo de validade expresso no documento, deverão ter sido emitidos há menos de 90 (noventa) dias da data estabelecida para o recebimento das propostas.

9.6.7. Em se tratando de microempresa ou empresa de pequeno porte, por ocasião da licitação, deverão apresentar toda a documentação exigida para efeito de comprovação fiscal, mesmo que esta apresente alguma restrição fiscal.

9.6.8. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado vencedor do certame, prorrogáveis por igual período, a critério da Administração, para regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa,conforme § 1° do Artigo 43 da Lei 123/2006 alterada pela Lei Complementar nº 155/2016.

9.6.9. A não regularização da documentação implicará decadência do direito à Contratação, sem prejuízo das sanções previstas no art. 90, §5º da Lei 14.133/2021, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para assinatura do Contrato, ou revogar a licitação.

10. DO JULGAMENTO DAS PROPOSTAS

10.1. Se a proposta ou o lance de menor valor não for aceitável, ou se o licitante desatender às exigências da habilitação, o pregoeiro examinará a proposta ou o lance subsequente, verificando a sua compatibilidade e a habilitação do participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o Edital. Também nessa etapa o pregoeiro poderá negociar com o participante para que seja obtido melhor preço.

10.2. Serão consideradas incompatíveis as propostas que:

a) apresentarem especificações ou condições em desacordo com o edital e anexos;

b) apresentarem preço global ou preço unitário superior ao respectivo preço estimado pela Administração no processo licitatório; ou preço manifestamente inexequível.

10.3. O(a) pregoeiro(a), observando-se o motivo do desatendimento das exigências da habilitação, aplicará as penalidades previstas neste Edital.

10.4. Constatando o atendimento das exigências fixadas neste Edital, o objeto será adjudicado ao autor da proposta ou lance de menor preço.

11. FASE RECURSAL

11.1. Qualquer licitante poderá, durante o **prazo de 10 (dez) minutos**, manifestar sua intenção de recorrer, de forma motivada, com a síntese de suas razões, em campo próprio do sistema. A falta de manifestação imediata e motivada da intenção de interpor recurso, via sistema eletrônico, implicará na decadência e preclusão desse direito, ficando a autoridade superior autorizada a adjudicar o objeto ao licitante declarado vencedor.

11.2. A recorrente deverá registrar, em campo próprio, as razões do recurso no **prazo de até 03 (três) dias**. Os interessados ficam, desde logo, intimados a apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo do recorrente.

11.3. Não será concedido prazo para recursos sobre assuntos meramente protelatórios ou quando não justificada a intenção de interpor o recurso pelo proponente.

11.4. Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

11.5. O acolhimento do recurso importará na invalidação apenas dos atos que não possam ser aproveitados.

11.6. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão, a qual poderá reconsiderar a decisão no prazo de 03 (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, contados do recebimento dos autos.

11.7. O recurso e pedido de reconsideração terão efeito suspensivo até a decisão final pela autoridade competente.

12. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

12.1. Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior para adjudicar o objeto e homologar o procedimento, observado o disposto no art. 71 da Lei nº 14.133/2021.

12.2 Após a adjudicação do objeto e a homologação do resultado da licitação pela autoridade competente, o licitante vencedor será convocado para assinar o termo de contrato ou para aceitar ou retirar o instrumento equivalente, dentro do prazo de **05 (cinco) dias úteis**, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital.

12.3. O prazo de vigência do presente contrato se inicia a partir da data de assinatura do mesmo, que ocorrerá no prazo máximo de **05 (cinco) dias**.

12.4. O prazo de convocação poderá ser prorrogado **01 (uma) vez**, por igual período, mediante solicitação da parte, durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

12.5. Será facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou não retirar o instrumento equivalente no prazo e nas condições estabelecidas neste Edital, convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.

12.6. Decorrido o prazo de validade da proposta indicado no item 7.6 deste Edital, sem convocação para a contratação, ficarão os licitantes liberados dos compromissos assumidos.

12.7. Na hipótese de nenhum dos licitantes aceitar a contratação, nos termos deste Edital, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

a) convocar os licitantes remanescentes para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário;

b) adjudicar e celebrar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

12.8. A recusa injustificada do adjudicatário em assinar o contrato ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas, previstas neste edital, e à imediata perda da garantia de proposta em favor do órgão licitante.

12.9. Não assinado o contrato no prazo anteriormente estipulado, a Administração poderá convocar os licitantes remanescentes, observada a ordem de classificação, para fazê-lo em igual prazo, após negociação, aceitação da proposta e comprovação dos requisitos de habilitação, celebrando com ele o compromisso representado pela assinatura do contrato, independentemente da cominação prevista no artigo 90 da Lei n.º 14.133/2021.

a) Após a publicação do contrato nos meios de comunicação da Prefeitura de Pedro Leopoldo, poderão ser solicitados os fornecimentos dentro do prazo de validade do Registro.

12.10. O(s) preço(s) e a indicação do(s) respectivo(s) fornecedor(es) serão divulgados no PNCP, nos meios de comunicação da Prefeitura de Pedro Leopoldo e disponibilizados durante toda a vigência do contrato.

12.11. Os licitantes que tenham seus adjudicados e homologados obrigar-se-ão a cumprir todas as condições dispostas no contrato.

12.12.O fornecimento será realizado de acordo com os pedidos feito ao prestador mediante solicitação, juntamente com a respectiva nota de empenho.

12.13. O fornecedor deverá manter, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, renovando as respectivas certidões, que, no caso de não poderem ser obtidas nos respectivos sítios dos órgãos emissores na internet, deverão ser encaminhadas a PMPL no prazo máximo de 48 (quarenta e oito) horas, a partir da solicitação das mesmas.

12.14. O prazo de vigência do contrato é de 60 (sessenta) meses, contados da data de assinatura do Contrato, prorrogável por até 15 anos , conforme artigo 106 e 114 da Lei nº 14.133, de 2021.

13. DA DOTAÇÃO ORÇAMENTÁRIA

13.1. A despesa decorrente do fornecimento relacionados neste processo correrá à conta da(s) seguinte(s) dotação(ões) do orçamento vigente:

132 - 02.05.05.04.126.0011.2039.3.3.90.40.00 - 5001.500.000 - RECURSOS NÃO VINCULADOS DE IMPOSTOS - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PESSOA JURÍDICA.

13.2. O custo total máximo estimado para a aquisição do objeto ora licitado é de R$498.568,20 (Quatrocentos e Noventa e Oito Mil Quinhentos e Sessenta e Oito Reais e Vinte Centavos)

14. DAS OBRIGAÇÕES DO(S) LICITANTE(S) VENCEDOR(ES)

14.1. Preparar e dotar de infraestrutura logística como contratação de software, link, pessoal de apoio, veículo, combustível, telefone e diárias para operacionalização dos serviços.

14.2. Cumprir rigorosamente todas as exigências estabelecidas neste Termo de Referência;

14.3. Realizar os serviços de acordo com as especificações;

14.4. Providenciar a imediata correção das irregularidades apontadas pela secretaria solicitante;

14.5. Garantir a boa qualidade dos serviços prestados, bem como o bom andamento dos jogos.

14.6. Responsabilizar-se por todos e quaisquer danos e/ou prejuízos que vierem causar à Secretaria solicitante ou a terceiros;

14.7. Comunicar ao município, no prazo de 24 horas, qualquer ocorrência anormal que impossibilite o cumprimento das obrigações assumidas.

14.8. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, garantindo sigilo e inviolabilidade das informações, respeitando as hipóteses constitucionais e legais de quebra de sigilo.

14.9. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Administração.

14.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

14.11. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

15. DOS CRITÉRIOS DE ATUALIZAÇÃO FINANCEIRA

15.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de 01 (um) ano contado da data do orçamento estimado para a presente contratação.

15.2. Após o interregno de 01 (um) ano, os preços iniciais serão reajustados, mediante a aplicação do Índice Nacional de Preços ao Consumidor Amplo – IPCA ou outro que houve por substituí-lo, caso mais favorável à Administração Pública, como critério de atualização monetária, nos termos do art. 25, §7º, da Lei nº 14.133/2021

15.3. A data-base estará vinculada à data do orçamento estimado e adjudicado ao licitante vencedor.

15.4. A extinção do contrato não configurará óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

15.5. O pedido de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação, nos termos do art. 107 e 131, parágrafo único, da Lei nº 14.133/2021.

15.6. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

15.7. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

15.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente.

15.9 O Contrato poderá ser rescindido nas hipóteses arroladas nos artigos 137 e 138 da Lei Federal nº 14.133/2021.

16. DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

16.1.1. 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;

16.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:
16.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

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

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

16.1.2.4. deixar de apresentar amostra;

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

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

16.1.3.1. 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;

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

16.1.5.fraudar a licitação;

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

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

16.1.6.3. induzir deliberadamente a erro no julgamento;

16.1.6.4. apresentar amostra falsificada ou deteriorada;

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

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

16.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

16.2.1. advertência;

16.2.2.multa;

16.2.3. impedimento de licitar e contratar e

16.2.4. 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.

16.3. Na aplicação das sanções serão considerados:

16.3.1. a natureza e a gravidade da infração cometida.

16.3.2. as peculiaridades do caso concreto

16.3.3. as circunstâncias agravantes ou atenuantes.

16.3.4. os danos que dela provierem para a Administração Pública.

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

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

16.4.1. Para as infrações previstas nos itens 16.1.1, 16.1.2. e 16.1.3, a multa será de 0,5% a 15% do valor do contrato licitado;

16.4.2. Para as infrações previstas nos itens 16.1.4, 16.1.5, 16.1.6., 16.1.7 e 16.1.8, a multa será de 15% a 30% do valor contrato licitado;

16.4.3. O valor da multa deverá observar o disposto no Art. 156, §1º da Lei 14.133/2021;

16.4.4. Conforme disposto no art.156 § 3º da Lei 14.133/2021 o percentual da multa aplicada nas infrações administrativas previstas no art. 155 seguirão a discricionariedade do gestor na fixação de multa, sendo os percentuais sugeridos meramente indicativos;

16.5. 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;

16.6. 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;

16.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 16.1.1, 16.1.2 e 16.1.3, 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, conforme estabelece o art.156,§ 4º da Lei 14.133/2021;
16.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 16.1.4, 16.1.5, 16.1.6, 16.1.7 e 16.1.8, bem como pelas infrações administrativas previstas nos itens 16.1.1, 16.1.2 e 16.1.3 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;

16.9. A recusa injustificada do fornecedor 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 , 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;

16.10. 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, conforme preceitua o art. 158 da Lei 14.133/2021.

16.11. 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, 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;

16.12. 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;

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

16.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados, conforme estabelece o art.156, §9º da Lei 14.133/2021;

17. DA EXECUÇÃO E GESTÃO

17.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e as condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este edital.

18. DO PAGAMENTO

18.1. A Prefeitura Municipal de Pedro Leopoldo promoverá o pagamento no prazo de 28 (vinte e oito) dias contados do recebimento da Nota Fiscal, devidamente certificada pela Secretaria solicitante.

18.2. As Notas Fiscais ou documentos que a acompanharem para fins de pagamento que apresentarem incorreções serão devolvidos à CONTRATADA e o prazo para o pagamento passará a correr a partir da data da reapresentação dos documentos, considerados válidos pelo CONTRATANTE.

18.3. É vedado à Contratada transferir a terceiros os direitos ou créditos decorrentes do contrato ou instrumento equivalente.

18.4. Nas Notas Fiscais deverão vir os dados bancários completos da CONTRATADA, sob pena de não realização do pagamento até a informação dos mesmos, de obrigação da CONTRATADA.

18.5. Para que os pagamentos possam ser efetuados, a contratada deverá apresentar, junto à nota fiscal de produtos, a seguinte documentação:

I - Documentos comprobatórios da regularidade fiscal e regularidade trabalhista;

18.6. Para que os pagamentos possam ser efetuados, a contratada deverá apresentar, junto a nota fiscal, os documentos comprobatórios da regularidade fiscal e regularidade trabalhista;

18.7.Sobre o valor devido ao contratado, a Administração efetuará as retenções tributárias cabíveis;

18.8. Quanto ao Imposto sobre Serviços de Qualquer Natureza (ISSQN), será observado o disposto na Lei Complementar Nº 116, de 2003, e legislação municipal aplicável.

19. DISPOSIÇÕES GERAIS

19.1. Na contagem dos prazos estipulados na presente licitação, excluir-se-á o dia do início e incluir-se-á o do vencimento.

19.2. A licitante e seu preposto são responsáveis pela fidelidade e legitimidade das informações e documentos apresentados em qualquer fase do processo licitatório.

19.3. Não havendo expediente ou correndo 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 do(a) Pregoeiro(a) em contrário.

19.4. Quaisquer textos ou documentos **redigidos em língua estrangeira** somente serão considerados válidos se acompanhados da respectiva tradução para língua portuguesa feita por tradutor juramentado, de acordo com o disposto no Decreto n.º 13.609/43, que regulamenta o ofício de tradutor público.

19.5. A Prefeitura Municipal de Pedro Leopoldo poderá revogar ou anular esta Licitação, nos termos do Art. 71 da Lei n.º 14.133/2021.

19.6. Qualquer medida judicial oriunda da presente licitação será processada na Comarca de Pedro Leopoldo, com expressa renúncia de outra, por mais privilegiada que seja.

19.7. **Durante a sessão a comunicação entre o (a) pregoeiro(a) e os licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.**

19.8. Será facultado o(a) Pregoeiro(a) ou autoridade superior, em qualquer fase do julgamento, promover diligência destinada a esclarecer ou complementar a instrução do processo.

19.9. Todas as decisões do(a) Pregoeiro(a) serão comunicadas mediante publicação no site desta Prefeitura, salvo com referência àquelas que puderem ser feitas diretamente às licitantes ou aos seus representantes legais.

19.10. O resultado da presente licitação estará disponível também na página da PMPL na internet, no seguinte endereço: http://www.pedroleopoldo.mg.gov.br.

19.11. O objeto deste Pregão poderá sofrer alterações, em conformidade com o art. 124 da Lei n.º 14.133/2021.

19.12. O(a) Pregoeiro(a), para fins de conferência, reserva-se o direito de exigir os originais de todos os documentos apresentados em fotocópias para esta licitação.

19.13. Para todas as referências de tempo contidas neste edital, será observado o horário de Brasília (DF).

19.14. Outros esclarecimentos sobre a presente licitação poderão ser obtidos, de segunda a sexta-feira, das 12 às 17h, pelo telefone: (31) 3660.5114, endereço de e-mail: licitacao@pedroleopoldo.mg.gov.br

19.15. Cópia do edital encontra-se à disposição dos interessados no site da Prefeitura www.pedroleopoldo.mg.gov.br e www.licitardigital.com.br.

19.16. OS INTERESSADAS EM PARTICIPAR DESTE PROCESSO, DEVERÃO FICAR ATENTAS À POSSÍVEIS ALTERAÇÕES DO EDITAL, CASO SEJAM NECESSÁRIAS, ATRAVÉS DE COMUNICADO NO SITE DESTA PREFEITURA – www.pedroleopoldo.mg.gov.br e www.licitardigital.com.br.

Pedro Leopoldo, 18 de novembro de 2024.

Kádma Diniz Araújo
Responsável pela elaboração do Edital

Raimundo Alves de Carvalho Mello Vianna
Gerente de Compras e Licitações

ANEXO I

TERMO DE REFERÊNCIA

ETP (x) sim ( ) não	Justificativa:

1. OBJETO E CONDIÇÕES GERAIS DE CONTRATAÇÃO:

1.1 Contratação de empresa especializada para prestação de serviços de segurança de rede de computadores composta por firewall com funcionalidades UTM (Unified Threat Management) incluindo serviços de suporte especializado.

1.2. O prazo de vigência da contratação é de 60 (sessenta) meses, contados da data de assinatura do Contrato, prorrogável por até 15 anos, conforme artigo 114 da Lei nº 14.133, de 2021.

> **Art. 114. O contrato que previr a operação continuada de sistemas estruturantes de tecnologia da informação poderá ter vigência máxima de 15 (quinze) anos.**

1.3. O quantitativo previsto para a contratação está detalhado no ANEXO I deste Termo de Referência.

2 . FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A contratação se fundamenta na necessidade de prover uma infraestrutura de rede de dados segura e eficiente, sendo por meio de equipamentos e softwares especializados, para que seja possível manter a integridade de todos os dados da Administração Pública Municipal, garantindo a segurança das informações. Além disso, assegura-se o funcionamento adequado e contínuo dos serviços de acesso à intranet e internet, com o devido controle e monitoramento da rede, dos usuários, dos sites acessados e dos arquivos maliciosos.

2.2. Firewalls são uma linha de defesa contra ataques externos, como hackers, malwares, ransomware e outras ameaças cibernéticas. Eles monitoram e controlam o tráfego de entrada e saída, bloqueando atividades suspeitas.

2.3. Em 2018 foi criada a Lei Geral de Proteção de Dados (Lei n.º 13.709, de 14 de agosto de 2018) que exige a proteção de dados e a segurança da informação. A contratação de um firewall ajuda a prefeitura a estar em conformidade com essas exigências legais, bem como proteger os dados e informações constantes em seu servidor.

2.4. Destacamos que com o aumento das ameaças cibernéticas, as Administrações Públicas de todos os tamanhos estão vulneráveis a ataques que podem resultar em perda de dados, interrupções operacionais e danos à Municipalidade, que um bom software de segurança, neste caso, software de firewall, oferece proteção abrangente, detecção e prevenção de intrusões,

antivírus e criptografia, além de atualizações automáticas e monitoramento em tempo real. Isso garante que o parque computacional esteja sempre protegida contra ameaças mais recentes .

2.5. Importante afirmar que Software Firewalls permitem a configuração de regras de acesso, garantindo que apenas pessoas autorizadas possam acessar determinadas áreas da rede. Isso é crucial para manter a segurança interna e evitar que funcionários ou terceiros acessem informações indevidas.

2.6. Investir em segurança da informação é uma necessidade estratégica para proteger dados sensíveis, manter a confiança dos cidadãos e cumprir regulamentações de privacidade, além de evitar custos elevados associados a violações de dados e interrupções operacionais.

2.7. Investir em segurança da informação é uma necessidade estratégica para proteger dados sensíveis, manter a confiança dos cidadãos e cumprir regulamentações e legislações de privacidade de dados, além de evitar custos elevados associados a violações de dados e interrupções operacionais da Administração Pública.

2.8. A contratação de uma empresa especializada em segurança da informação pelo prazo de 60 meses fundamenta-se na natureza contínua dos serviços prestados, além de serviços estruturantes de Tecnologia da Informação, sendo indispensáveis para garantir a proteção e a integridade dos ativos digitais e das informações estratégicas da instituição em tempo integral.

2.8.1. Os serviços de segurança da informação englobam atividades críticas e de caráter permanente, como:

2.8.1.1. Monitoramento contínuo de sistemas e redes para detecção e resposta a ameaças cibernéticas em tempo real.

2.8.1.2. Gestão de vulnerabilidades, incluindo a realização periódica de análises de riscos, testes de invasão (pentests) e implementação de correções.

2.8.1.3. Atualização e manutenção de ferramentas de segurança, como firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS), e soluções de antivírus e antimalware.

2.8.1.4. Conformidade regulatória, assegurando que a instituição atenda às normas e legislações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD).

2.8.1.5. Capacitação e conscientização dos colaboradores, com treinamentos regulares sobre boas práticas de segurança e proteção contra phishing e outras ameaças.

2.8.2. Devido à complexidade e à criticidade desses serviços, é imprescindível garantir sua execução de maneira ininterrupta e com a qualidade necessária, o que demanda um contrato de longo prazo com uma empresa especializada. Esse modelo permite:

2.8.2.1. Continuidade operacional, evitando interrupções que poderiam comprometer a segurança e o

desempenho dos sistemas.

2.8.2.2. Economia de escala, ao firmar um contrato estendido com condições favoráveis de investimento em soluções tecnológicas e especializadas.

2.8.2.3. Planejamento estratégico, permitindo maior previsibilidade e alinhamento das ações de segurança ao planejamento de longo prazo da instituição.

2.8.3. Além disso, o prazo de 60 meses é adequado para a maturação e aprimoramento contínuo das estratégias e processos de segurança, considerando a rápida evolução das ameaças cibernéticas e das tecnologias de proteção.

2.8.4. Assim, justifica-se a contratação pelo período proposto como medida essencial para assegurar a proteção contínua das informações e a conformidade da instituição com as melhores práticas e exigências do mercado.

2.9. A presente contratação se encontra alinhada com o Plano Anual de Contratação.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

3.1. A prestação de serviço de firewall com funcionalidades UTM (Unified Threat Management) para a prefeitura de Pedro Leopoldo, incluindo serviços de suporte especializado, será essencial para garantir a segurança e a eficiência da infraestrutura de rede. Esse processo envolverá várias etapas críticas, começando pela implementação e configuração.

3.1.1.Inicialmente, a instalação física do hardware UTM será realizada no Data Center de TI, na Sede Municipal, em seguida pela implementação do software UTM e sua integração com a infraestrutura de rede existente. A configuração das políticas de segurança será um passo crucial, onde serão criadas e ajustadas regras de firewall, perfis de antivírus, filtragem de URL, controle de aplicativos e configurações de VPN para atender às necessidades específicas da prefeitura.

3.1.2.Após a configuração inicial, serão realizados testes de funcionamento para assegurar que todas as funcionalidades do UTM estarão operando corretamente. A eficácia das políticas de segurança implementadas será verificada, e ajustes serão feitos conforme necessário para otimizar a segurança e o desempenho da rede.

3.1.3.O monitoramento contínuo da rede será fundamental para garantir a segurança em tempo real. O tráfego de rede e os eventos de segurança serão monitorados constantemente utilizando as funcionalidades UTM, com o auxílio de dashboards e alertas em tempo real para identificar e responder a ameaças rapidamente. Atualizações regulares de software e firmware serão aplicadas para manter a proteção contra novas vulnerabilidades e ameaças, incluindo a manutenção das assinaturas de antivírus e antimalware atualizadas.

3.1.4.O suporte técnico especializado desempenhará um papel vital nesse processo. Disponível de forma proativa, o suporte técnico resolverá problemas e otimizará o desempenho do UTM, além de identificar e resolver potenciais problemas de segurança. Em caso de incidentes de segurança, procedimentos estabelecidos garantirão uma resposta rápida, incluindo análise forense, mitigação de ameaças e restauração de serviços.

3.1.5.A auditoria e revisão periódica das medidas de segurança serão essenciais para avaliar a eficácia das políticas implementadas e identificar áreas de melhoria. Auditorias regulares serão realizadas para avaliar a segurança, e relatórios detalhados sobre o desempenho do UTM, incidentes de segurança e medidas tomadas serão gerados. Análises de tendências ajudarão na elaboração de estratégias para melhoria contínua.

3.1.6.O treinamento e a capacitação dos funcionários serão igualmente importantes para a manutenção de uma rede segura. Programas de treinamento contínuos educarão os funcionários sobre as melhores práticas de segurança e o uso seguro da rede, enquanto a equipe de TI receberá capacitação específica sobre a administração e utilização eficaz da solução UTM. A atualização contínua do conhecimento da equipe de TI sobre novas tecnologias, ameaças emergentes e técnicas avançadas

de segurança cibernética será fundamental para enfrentar os desafios em constante evolução na área de segurança da informação.

3.2.A implementação de um serviço de firewall com funcionalidades UTM e suporte especializado para a prefeitura de Pedro Leopoldo garantirá uma defesa robusta e abrangente contra ameaças cibernéticas. Esse serviço assegurará a proteção dos dados municipais e a continuidade dos serviços essenciais, com suporte técnico especializado e revisões periódicas contribuindo para a manutenção e melhoria contínua da segurança da rede.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos técnicos:

4.1.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.0 Gbps ou superior.

4.1.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

4.1.3. Desempenho mínimo de 3.3 Gbps de IPS.

4.1.4. Suporte mínimo de 500.000 conexões simultâneas/concorrentes no modo DPI.

4.1.5. Suporte mínimo de 20.000 novas conexões por segundo.

4.1.6. Deve suportar expansão de armazenamento interno para até 256Gb.

4.1.7. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

4.1.8. Deve possuir 16 interfaces 1 GbE padrão RJ-45.

4.1.9. Deve possuir 3 interfaces 10GbE SFP+; Deve possuir 1 do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.

4.1.10. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

4.1.11. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos, com aquisição de licença complementar.

4.1.12. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 100 usuários simultâneos, com aquisição de licença complementar.

4.1.13. Deve suportar 250 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

4.1.14. Deve suportar, no mínimo, 2.1 Gbps de desempenho de VPN IPSEC.

4.1.15. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

4.1.16. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

4.1.17. O Equipamento deverá ser homologado pela ANATEL.

4.1.18. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

4.1.19. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 12(doze) meses, renováveis de acordo com o prazo da prestação e execução dos serviços.

4.1.20. A garantia do hardware deverá ser de 12 (doze) meses.

4.1.21. É imprescindível que a solução possua um limite mínimo de tamanho de arquivos de, ao menos, 400Mb, no uso da tecnologia 'gateway antimalware' liveprotection, já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

4.2.Características Gerais Dos Firewalls Físicos

4.2.1.Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

4.2.2.Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

4.2.3.A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

4.2.4.Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.

4.2.5.Não serão aceitas soluções baseadas em PCs (personal computers) de uso geral, assim como soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

4.2.6.Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 12(doze) meses, incluindo garantia e suporte, renováveis de acordo com o prazo da prestação e execução dos serviços.

4.3.Características Diversas

4.3.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

4.3.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do túnel IPSec.

4.3.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

4.3.5. Deve possuir proteção anti-spoofing.

4.3.6. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP.

4.3.7. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

4.3.8. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

4.3.9. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

4.3.10. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

4.3.10.1. Latência;

4.3.10.2. Jitter;

4.3.10.3. Perda de pacotes.

4.3.11. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico.

4.3.12. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

4.3.13. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

4.3.14. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

4.3.15. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

4.3.16. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

4.3.17. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

4.3.18. Deve suportar DHCP relay.

4.3.19. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

4.3.20. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.

4.3.21. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares P2P (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

4.3.22. Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

4.3.23. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

4.3.24. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

4.3.25. Detectar e bloquear a origem de portscans.

4.3.26. Deve permitir o bloqueio de ataques.

4.3.27. Deve permitir o bloqueio de exploits conhecidos.

4.3.28. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP.

4.3.29. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação.

4.3.30. Implementar DSCP (Differentiated Services Code Points).

4.3.31. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

4.3.32. Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice Over IP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

4.3.33. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

4.3.34. Possuir suporte ao protocolo SNMP versões 2 e 3.

4.3.35. Possuir suporte a log via syslog.

4.3.36. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

4.3.37. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

4.3.38. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.

4.3.39. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

4.3.40. Para tráfego criptografado SSL/TLS, deve decriptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

4.3.41. Controle, inspeção e decriptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.

4.3.42. Deve permitir a funcionalidade de ARP bridging.

4.3.43. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm".

4.4 **Características De VPN**

4.4.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

4.4.2. Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256

4.4.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

4.4.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

4.4.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

4.4.6. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

4.4.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

4.4.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

4.4.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

4.4.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

4.4.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

4.4.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

4.4.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

4.4.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

4.4.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

4.4.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

4.5. **Alta Disponibilidade**

4.5.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

4.5.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover.

4.5.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

4.5.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

4.5.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

4.5.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

4.5.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

4.5.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

4.5.9. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

4.6. **Controle De Ameaças**

4.6.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

4.6.2. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

4.6.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

4.6.4. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

4.6.5. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

4.6.6. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

4.6.7. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

4.6.8. Implementar interface CLI segura através do protocolo SSH.

4.6.9. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

4.6.10. A solução deve permitir criar regras de exceção de acordo com a proteção.

4.6.11. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

4.6.12. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

4.6.13. A solução deve ser capaz de proteger contra ataques a DNS.

4.6.14. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

4.6.15. A solução deve ser capaz de prevenir acesso a websites maliciosos.

4.6.16. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

4.6.17. A solução deverá receber atualizações de um serviço baseado em cloud.

4.6.18. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

4.6.19. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

4.6.20. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

4.6.21. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.

4.6.22. A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

4.7. Proteção Contra Ataques Avançados

4.7.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

4.7.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

4.7.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

4.7.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

4.7.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

4.7.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

4.7.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

4.7.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

4.7.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

4.7.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este

4.8. **Características De Filtro De Conteúdo Web**

4.8.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.

4.8.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local.

4.8.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.

4.8.4. Permitir a customização de página de bloqueio.

4.8.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

4.8.6. Deve permitir submissão de novos sites para categorização.

4.8.7. Permitir a classificação dinâmica de sites web, URLs e domínios.

4.8.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

4.8.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

4.8.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

4.9. Características De Autenticação

4.9.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

4.9.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

4.9.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

4.9.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

4.9.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

4.9.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW.

4.9.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

4.9.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

4.9.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

4.9.10. A solução deve possibilitar SSO via API

4.10. Características De Administração

4.10.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

4.10.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

4.10.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

4.10.4. Possuir mecanismo para agendamento realização das cópias de segurança (backups) de configuração.

4.10.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

4.10.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

4.10.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.

4.10.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.

4.10.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

4.10.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de "ICMP Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCP-Reset" para o servidor ou para os dois lados da conexão.

4.10.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

4.10.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real, estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

4.10.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

4.10.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.

4.10.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

4.10.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

4.10.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

4.10.18. Ser capaz de implementar a funcionalidade de "Zero-Touch", permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

4.10.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

4.10.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

4.10.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

4.10.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

4.10.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

4.10.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

4.10.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

4.10.26. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto-provisionamento da plataforma através de ponto central de gerenciamento.

4.10.27. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações.

4.10.28. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.

4.10.29. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

4.11 Gerenciamento Unificado e Relatórios

4.11.1. Deve possuir solução de gerenciamento centralizado em nuvem do mesmo fabricante, para gerenciamento de toda solução.

4.11.2. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções dos usuários da console que determinem usuários

a. Grupos de firewalls permitidos

b. Funcionalidades permitidas por firewall ou grupo de firewalls de acordo com o perfil de uso designado

c. Perfil de nível de acesso (escrita, leitura, administração, relatórios)

4.11.3. Deve suportar organizar os dispositivos administrados em grupos. Estes grupos devem permitir isolamento tanto de acesso para os administradores como de configuração massiva ou individual

4.11.4. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls.

4.11.5. Deve apresentar estado dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

4.11.6. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

4.11.7. O gerenciamento deve permitir/possuir:

a. Criação e administração de políticas de firewall e controle de aplicação

b. Monitoração de logs;

c. Investigação de evendos de segurança e falhas (debugging)

d. Acesso concorrente de administradores, conforme políticas e perfis previamente definidos

4.11.8. Deve permitir o provisionamento e configuração sem intervenção de operadores (Zero-Touch). Os firewalls devem se conectar automaticamente à plataforema de gerencia, e à partir desta conexão receberem as configurações previamente determinadas pelos operadores da plataforma.

4.11.9. A solução de gerenciamento deve ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL

4.11.10. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

4.11.11. A solução deve possuir tela situacional com todo os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador:

a. nome do firewall

b. número de série

c. modelo

d. versão do firmware e estado da conectividade do equipamento com a gerência em online ou offline.

4.11.12. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;

4.11.13. Deve centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento, possibilitando comparação de configurações que evitem sobreposição de regras e conflitos de configuração.

4.11.14. A solução deve possuir Dashboard com sumario de alertas e informação de status de licença

4.11.15. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo

4.11.16. Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência

4.11.17. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN

4.11.18. A solução deve permitir a criação de modelos de configuração (templates) para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls

4.11.19. A solução deve possibilitar a geração de templates de configuração à partir da configuração vigente em um firewall selecionado pelo administrador da plataforma, e possibilitar que este template possa ser editado e utilizado em outros firewalls gerenciados pela plataforma.

4.11.20. Os modelos de configuração (templates) devem suportar configurações de interfaces físicas ou virtuais

4.11.21. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

4.11.22. Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas.

4.11.23. De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento;

4.11.24. Deve incluir console de configuração e monitoramento SD-WAN, possibilitar a criação de políticas SD-WAN em todos os elementos gerenciados, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

4.11.25. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

4.11.26. Durante a alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

4.11.27. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, este processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente

4.11.28. A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.

4.11.29. A solução deve oferecer monitor de auditoria de configuações aplicadas aos firewalls gerenciados pela plataforma, permitindo comparativo diferencial entre registros para rápida identificação de configurações e alterações aplicadas.

4.11.30. A solução deve oferecer módulo centralizado que possibilite realização e armazenamento de backup de configurações dos firewalls gerenciados.

4.11.31. A solução deve oferecer possibilidade de auditoria de configurações.

4.11.32. A solução deve possibilitar o monitoramento em tempo real dos firewalls gerenciados, informando minimamente:

4.11.33.a. Utilização de CPU/Processamento

b. Aplicações em uso e seu consumo de banda

c. Interfaces em uso e utilizaçào de banda

d. Conexões concorrentes em uso

4.11.34. A solução deverá permitir visualizar sumario com as informações referentes as principais ameaças protegidas pelos firewalls

4.11.35. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a geração de relatórios e monitoramento em tempo real.

4.11.36. A solução deverá prover relatórios com no mínimo histórico de 365 dias

4.11.37. A solução deverá prover relatórios referente as atividades dos usuários

4.11.38. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações:

a. nome da aplicação

b. quantidade de conexões

c. percentual que a aplicação representa do tráfego da rede e quantidade de Megabytes trafegados

4.11.39. A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações:

a. nome do usuário

b. quantidade de conexões

c. percentual que tráfego do usuário representa na rede

d. quantidade de Megabytes trafegados

4.11.41. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações:

a. endereço IP

b. quantidade de conexões

c. percentual que tráfego que o IP representa na rede

d. quantidade de Megabytes trafegados

4.11.42. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede

4.11.43. A solução deverá arquivar relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF

4.11.44. A solução deverá permitir geração e envio agendado de relatórios

4.11.45. A solução deve permitir a customização de alertas e notificações, possibilitando o envio de e-Mail com as informações relativas a este evento.

4.11.46. A solução deve possibilitar configuração e monitoramento centralizados de VPNs entre os firewalls gerenciados

4.11.47. A solução deve apresentar consoles de indicação com os principais eventos, riscos e ameaças contendo:

a. Aplicações de maior risco, e volume de dados consumido por estas

b. Aplicações de maior utilização, por volume de dados transferidos e conexões consumidas

c. Aplicações de maior utilização, por categoria

4.11.48. A solução deve apresentar consoles de indicação dos principais usuários contendo:

4.11.49. a. Usuários utilizando mais conexões

4.11.48. b. Usuários consumindo mais dados

4.11.50. A solução deve apresentar console de indicação de:

a. Virus/Spyware blockeados

b. Intrusões bloqueadas

c. Botnets bloqueados

d. Origens e destinos mais utilizados

4.11.51. A solução deve apresentar console de indicação de Aplicações indicando:

a. Aplicações identificadas

b. Categorização e uso das aplicações

c. Risco das aplicações

4.11.52. A solução deve permitir visualização de eventos correlacionados que possam ser investigados por:

a. Lista de eventos correlacionados com opção de navegação "drilldown"; ou

b. Modo gráfico; ou

c. Lista de logs

4.11.53. A solução deve apresentar console de monitoramento de produtividade dos usuários, indicando suas características de navegação de acordo com políticas previamente estabelecidas e categorizadas como:

a. Produtivas

b. Não produtivas

c. Aceitáveis para a política de uso corporativa

d. Inaceitáveis para a política de uso corporativa

e. Customizadas

4.11.54. A solução deve permitir visualização de topologia do firewal e elementos a ele conectados (dispositivos de rede complementares, dispositivos de usuários, Access Points)

4.11.55. O Fabricante deverá comprovar que possui tecnologia holística capaz de integrar suas principais soluções em uma base centralizada gráfica com informações e alertas, comprovando integração de pelo menos 2 de suas plataformas de segurança.

4.12. **Treinamento de Capacitação:**

4.12.1.Deverá ser realizado um treinamento para solução integrada de Firewall e Service Gateway a ser utilizada na prestação dos serviços, ministrado por profissional certificado na solução. Este será realizado na Prefeitura para até 8 (oito) pessoas em uma única turma. A duração deverá ser de no mínimo 16 (dezesseis) horas, abordando as os seguintes tópicos:

- Introdução à plataforma e funcionalidades do equipamento;

- Introdução ao software de gerenciamento;
- Introdução à interface gráfica de usuário;
- Regras de Firewall;
- Zonas de segurança;
- Políticas de segurança;
- Autenticação de usuários;
- Proteção de rede;
- NAT (Network Addres Translation).

4.12.2.O treinamento deve ser vinculado as plataformas vencedoras do item 1;

4.12.3.Qualquer despesa incorrida tais como escopo do serviço, passagens aéreas, locação de veículos, hospedagens e alimentação do instrutor será de responsabilidade exclusiva do contratado.

4.12.4.Será de responsabilidade da Prefeitura a disponibilização de infraestrutura e dos equipamentos para montagem da sala de aula e laboratório.

4.12.5.Os treinamentos serão ministrados no idioma português. Os materiais fornecidos podem estar no idioma português ou inglês.

4.12.6.Após a realização do treinamento, deverá ser fornecido um certificado formal de participação para cada participante do evento.

4.12.7.A proponente vencedora deverá apresentar, durante a sessão do pregão, catálogo ou manual impresso publicado pelo fabricante do equipamento ofertado, em língua portuguesa ou inglesa, com identificação precisa da página onde se encontram as informações sobre o atendimento de cada requisito exigido na especificação técnica;

4.12.8.Poderá ser aceita cópia de documento publicado no sítio do fabricante na Internet que comprove as especificações do equipamento, desde que da mesma conste o endereço eletrônico de acesso irrestrito, devendo estar disponível para acesso ao público em geral e passível de verificação durante a sessão do pregão.

4.12.9.Todas as declarações deverão ser apresentadas com firma reconhecida em cartório e acompanhadas dos documentos que comprovem a capacidade legal de quem as assinou;

4.12.10.Todos os documentos deverão estar vigentes no dia previsto para realização deste pregão.

4.13. Sustentabilidade:

4.13.1. A presente aquisição não possui relevantes impactos ambientais, contudo, os licitantes deverão ofertar, no que couber, visando a atender ao disposto na legislação aplicável, a CONTRATADA deverá priorizar, para o fornecimento do objeto, a utilização de bens que sejam no todo ou em parte compostos por materiais recicláveis, atóxicos e biodegradáveis.

4.14. Da Visita Técnica

4.14.1. Para o correto dimensionamento e elaboração de sua proposta, é facultado ao licitante realizar visita técnica ao local de execução dos serviços. A visita técnica, quando realizada, deverá ser acompanhada pelo responsável técnico da Divisão de T.I.

4.14.2. As vistorias técnicas poderão ser realizadas de segunda à sexta-feira, no horário entre 09:00 horas às 17:00 horas, devendo o agendamento ser efetuado previamente pelo telefone (31) 3660-5122 ou através do e-mail ti@pedroleopoldo.mg.gov.br.

4.14.3. Realizada a visita técnica, será emitida uma Declaração de Vistoria Técnica, conforme modelo constante do Anexo II, a Declaração de Visita Técnica comprovará que a empresa tomou ciência de todas as informações necessárias para a execução do objeto em questão.

4.14.4. Caso a licitante opte pela não realização da vistoria técnica, esta não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante, caso seja vencedora, assumir os ônus dos serviços decorrentes; e optado pela não realização da vistoria técnica, será emitida uma Declaração de Dispensa de Visita Técnica, conforme modelo constante do Anexo III.

4.15. Do Suporte, Garantia e Assistência Técnica:

4.15.1. Todos os serviços de suporte e manutenção preventiva ou corretiva, assim como a substituição de peças e suprimentos necessários ao perfeito funcionamento do bem durante a vigência do contrato, serão prestados pelo fornecedor.

4.15.2. O suporte técnico será realizado remoto ou "on-site", de acordo com a necessidade e requisição da Prefeitura, sem ônus adicional durante a vigência do contrato.

4.15.3. A Contratada deverá disponibilizar um aplicativo via web para abertura de chamados de suporte técnico, ou Central de Atendimento ou correio eletrônico do prestador de serviços;

4.15.4. O prazo de atendimento para solução deverá ser respeitado de acordo com a tabela de prioridades e prazos abaixo:

Serviços	**Prioridade**	**Prazo**
Atendimento Telefônico	**1,2 e 3**	24x7 (24 Horas / 7 Dias Semana)

Abertura de Chamados WEB		
Horário de Atendimento	**1,2 e 3**	24x7 (24 Horas / 7 Dias Semana)
Tempo de Resposta para Serviços Remotos	**2**	Até 2 Horas Úteis
	3	Até 4 Horas Úteis
Atendimentos “On Site”	**1**	Até 4 Horas Úteis

Descrição das Prioridades:

1 - Não conformidades que restringem completamente (80 a 100%) o funcionamento de todo o sistema ou apresentem-se como ameaças concretas. *Ex.:* Paralisação do Firewall ou da rede WAN.

2 - Não conformidades que restringem parcialmente (26 a 80%) o funcionamento de todo o sistema ou apresentam-se como vulnerabilidades para possíveis ameaças. *Ex.:* Lentidão na performance

3 - Não conformidades que não restringem (0 a 25%) o funcionamento de todo o sistema, mas sim de usuários isolados *Ex.:* Um usuário bloqueado

5. MODELO DE EXECUÇÃO CONTRATUAL .

5.1. O prazo de entrega e início da prestação dos serviços (incluindo instalação, configuração do equipamento e capacitação da solução entregue), se dará em até 60 (sessenta) dias corridos, contados a partir do recebimento pelo fornecedor da Ordem de serviços

5.2. A CONTRATADA deverá informar à CONTRATANTE, quando da entrega dos equipamentos com, no mínimo, 10 (dez) dias corridos de antecedência, ficando a CONTRATADA responsável pelo transporte e entrega de equipamentos e/ou partes componentes da solução integrada de segurança da informação.

5.3. A Ordem de serviço ou de fornecimento de bens indicará a quantidade, os endereços de entrega e da instalação e nome do responsável pelo recebimento, acompanhado de e-mail e/ou telefone para contato.

5.4. A montagem e a instalação dos equipamentos deverão ser feitas pelo fornecedor, não sendo aceito a terceirização dos serviços no local de entrega e em horários a serem agendados pela Divisão de Tecnologia da Informação da Prefeitura, na sede da Prefeitura Municipal de Pedro Leopoldo, localizada à Rua Dr Cristiano Otoni, 555, Centro.

5.5. Não será permitida a subcontratação do objeto dessa contratação

5 .6. A assistência técnica e suporte deverão ser prestados por profissionais especializados, com certificados devidamente emitidos, com experiência nos serviços e produtos que compõem a solução, assim como recursos ferramentais necessários, disponibilizados pela CONTRATADA, para a prestação dos serviços.

5.7. Mediante termo aditivo, e de acordo com a capacidade operacional do CONTRATADO, o CONTRATANTE poderá, nos termos da Lei Federal nº 14.133/21 e considerando suas necessidades, fazer acréscimos ou supressões nos valores limites desse contrato, durante o período de sua vigência, incluídas as prorrogações, por meio de solicitação justificada do Secretário Municipal de Administração ou outra autoridade competente.

6. DA GESTÃO E FISCALIZAÇÃO DO CONTRATO:

6.1.O contrato ou instrumento equivalente deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. A execução do contrato ou instrumento equivalente deverá ser acompanhada e fiscalizada pelo(s) fiscal(is), ou pelos respectivos substitutos.

6.3. O contrato ou instrumento equivalente oriundo desta contratação terá como responsáveis:

6.3.1. GESTOR:

- Hélder Sebastião dos Santos- Secretário Municipal de Administração;

6.3.2. FISCAIS:

- Alexandre Thadeu Clemenete Bassouto - Analista de Sistemas e Redes III - Fiscal Técnico - Titular
- Paula Poliana Gonçalves Braga- Assistente Administrativo II - Fiscal Administrativo - Titular
- Victor Hugo Pereira Reis - Gerente de Tecnologia da Informação - Fiscal Administrativo/Técnico - Substituto Titular

6.3.2.1 O fiscal do contrato ou instrumento equivalente anotará em registro próprio todas as ocorrências relacionadas à execução, determinando o que for necessário para a regularização das faltas ou dos defeitos observados.

6.3.2.2. O fiscal do contrato ou instrumento equivalente informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência.

6.4. O contratado será obrigado a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato ou instrumento equivalente em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados.

6.5. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato ou instrumento equivalente, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante.

6.6. Somente o contratado será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato ou instrumento equivalente.

6.6.1. A inadimplência do contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato ou instrumento equivalente.

6.7. As comunicações entre a Administração e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, excepcionalmente, o uso de mensagem eletrônica para esse fim.

6.8. A Administração poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.9. Antes do pagamento da nota fiscal ou da fatura, deverá ser consultada pela Secretaria Municipal de Fazenda do Município, a situação da empresa junto ao Cadastro de Fornecedores do Município – CFM.

6.9.1. Serão exigidos a Certidão Negativa de Débito (CND) relativa a Créditos Tributários Federais e à Dívida Ativa da União, o Certificado de Regularidade do FGTS (CRF), a Certidão Negativa de Débito Municipal e a Certidão Negativa de Débitos Trabalhistas (CNDT), caso esses documentos não estejam regularizados no CFM.

7. FORMA E CRITÉRIOS DE SELEÇÃO:

7.1. A forma de contratação será através de procedimento licitatório na modalidade Pregão Eletrônico.

7.2. O critério de julgamento será o de Menor preço por lote único.

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

8.1. Para estimativa dos valores a serem contratados utilizou-se como base no Estudo Técnico Preliminar, apêndice deste Termo de Referência, o contrato vigente de número 018-2022 - MGSOFT Comércio e Serviços em Tecnologia da Informação Ltda – ME). Os valores encontram-se descritos no Anexo IV deste documento.

8.2. O custo unitário estimado da contratação, baseado na pesquisa de preços realizada para composição do processo, possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas, conforme previsto no artigo 24 da Lei Federal nº 14.133/21, nos seguintes termos:

> **Art. 24 Desde que justificado, o orçamento estimado da contratação poderá ter caráter sigiloso, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas.**

8.3. Para o objeto desta licitação, manter o sigilo sobre o orçamento estimado incentiva a apresentação de propostas mais vantajosas e põe em prática os princípios fundamentais da competitividade, eficiência e economicidade O sigilo visa evitar que o preço de referência estabelecido pela Administração influencie o alinhamento das propostas apresentadas e incentiva os interessados a apresentem preços competitivos que fomentem o ambiente de concorrência. Vale destacar o efeito prático do sigilo do orçamento, com reflexos positivos ao propósito de alcançar potencial vantagem no processo competitivo. A não publicação dos valores estimados da contratação, afasta a participação de propostas aventureiras, confeccionadas sem expertise, com menor capacidade de planejamento, que habitualmente utilizam o preço estimado pela Administração como parâmetro, aplicando apenas um percentual de redução dos valores, muitas vezes, sem um trabalho técnico e responsável.

9. DOS CRITÉRIOS TÉCNICOS DE HABILITAÇÃO

9.1. Como critério de habilitação deverão ser apresentados os seguintes documentos:

9.1.1. Apresentação de atestado(s) emitido(s) por pessoa(s) jurídica(s), de direito público ou privado, que comprove(em) a execução, pela contratada, de serviços compatíveis com o objeto licitado, conforme discriminação contemplada neste documento.

9.1.2. A empresa prestadora dos serviços deverá possuir em seu quadro de funcionários ou sócios o mínimo de 01 (um) técnico certificado pelo fabricante, comprovado através da apresentação de cópia do certificado válido emitido pelo fabricante do produto

10. OBRIGAÇÕES DO CONTRATADO:

10.1. Preparar e dotar de infraestrutura logística como contratação de software, link, pessoal de apoio, veículo, combustível, telefone e diárias para operacionalização dos serviços.

10.2. Cumprir rigorosamente todas as exigências estabelecidas neste Termo de Referência;

10.3. Realizar os serviços de acordo com as especificações;

10.4. Providenciar a imediata correção das irregularidades apontadas pela secretaria solicitante;

10.5. Garantir a boa qualidade dos serviços prestados, bem como o bom andamento dos jogos.

10.6. Responsabilizar-se por todos e quaisquer danos e/ou prejuízos que vierem causar à Secretaria solicitante ou a terceiros;

10.7. Comunicar ao município, no prazo de 24 horas, qualquer ocorrência anormal que impossibilite o cumprimento das obrigações assumidas.

10.8. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, garantindo sigilo e inviolabilidade das informações, respeitando as hipóteses constitucionais e legais de quebra de sigilo.

10.9. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Administração.

10.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

10.11. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

11. OBRIGAÇÕES DO MUNICÍPIO:

11.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o descrito neste Termo de Referência;

11.2. Receber o objeto no prazo e condições estabelecidas;

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

11.4. Acompanhar e fiscalizar a execução do contrato ou instrumento equivalente e o cumprimento das obrigações pelo Contratado, através de servidor especialmente designado;

11.5. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Termo de Referência;

11.6. Aplicar ao Contratado sanções motivadas pela inexecução total ou parcial do objeto;

11.7. Cientificar o NUPAD - Núcleo de Procedimento para Apuração de Descumprimento de Cláusulas Contratuais (NUPAD), no endereço eletrônico nupad@pedroleopoldo.mg.gov.br, para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

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

12. AFERIÇÃO E PAGAMENTO:

12.1. A Prefeitura Municipal de Pedro Leopoldo promoverá o pagamento no prazo de 28 (vinte e oito) dias contados do recebimento da Nota Fiscal, devidamente certificada pela Secretaria solicitante.

12.2. As Notas Fiscais ou documentos que a acompanharem para fins de pagamento que apresentarem incorreções serão devolvidos à CONTRATADA e o prazo para o pagamento passará a correr a partir da data da reapresentação dos documentos, considerados válidos pelo CONTRATANTE.

12.3. Nas Notas Fiscais deverão vir os dados bancários completos da CONTRATADA, sob pena de não realização do pagamento até a informação dos mesmos, de obrigação da CONTRATADA.

12.3.1 Para que os pagamentos possam ser efetuados, a contratada deverá apresentar, junto à nota fiscal de produtos, a seguinte documentação:

I - Documentos comprobatórios da regularidade fiscal e regularidade trabalhista;

12.4. Sobre o valor devido ao contratado, a Administração efetuará as retenções tributárias cabíveis.

12.5. Quanto ao Imposto sobre Serviços de Qualquer Natureza (ISSQN), será observado o disposto na Lei Complementar Nº 116, de 2003, e legislação municipal aplicável.

12.6. É vedado ao contratado transferir a terceiros os direitos ou créditos decorrentes do contrato ou instrumento equivalente.

13. ADEQUAÇÃO ORÇAMENTÁRIA:

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Municipal.

13.2. A contratação será atendida pelas seguintes dotações orçamentárias:

Secretaria	Fichas	Fonte
Administração	132	1500

Pedro Leopoldo, 06 de Agosto de 2024

_____

Natália de Sousa Arcanjo Martins

Responsável pela elaboração do Termo de Referência

_____

Victor Hugo Pereira Reis

Responsável Técnico pela elaboração do Termo de Referência

Fiscal do Contrato (Substituto)

_____

Alexandre Thadeu Clemenete Bassouto

Responsável Técnico

Fiscal Técnico do Contrato

_____

Paula Poliana Gonçalves Braga

Fiscal Administrativo do Contrato

Pedro Leopoldo, 06 de Agosto de 2024.

APROVO ESTE TR E DECLARO QUE TENHO CONHECIMENTO DE TODAS AS SUAS CARACTERÍSTICAS, RATIFICANDO, NESTE ATO, O SEU INTEGRAL CONTEÚDO

_____

Hélder Sebastião Santos

Secretário Municipal de Administração

Gestor do Contrato

ANEXO I

SOFTWARE DE SEGURANÇA DA INFORMAÇÃO

ITEM	DESCRIÇÃO	UNIDADE MEDIDA	QUANTIDADE
1.	Contratação de empresa especializada em prestação de serviços de segurança da Informação, incluindo equipamentos UTM necessários para prestação dos serviços, monitoramento e suporte especializado em modalidade 24x7, incluindo instalação de equipamentos, configuração, documentação e capacitação de no mínimo 16 (dezesseis) horas aos servidores da Divisão de Tecnologia da Informação.	Mês	60 meses

ANEXO II

DECLARAÇÃO DE VISITA TÉCNICA

Declaramos, para fins de participação no Pregão Eletrônico nº ..... /....., que a empresa..... (nome ou razão social da empresa) ....., CNPJ/MF n.º....., representada por seu Responsável Técnico..... (nome do responsável) ....., CPF nº....., em visita realizada às instalações da Prefeitura Municipal de Pedro Leopoldo, está ciente das condições atuais de infraestrutura, bem como das quantidades, marcas e configurações dos equipamentos de informática e ainda dos softwares em utilização pela instituição, e que recebeu instruções e informações adicionais necessárias ao atendimento do objeto e demais condições do Edital, não havendo, portanto, nenhuma dúvida que prejudique a apresentação de uma proposta completa e com todos os detalhes.

Declaramos ainda, que a supramencionada empresa está ciente do compromisso assumido de manter sigilo sobre todas as informações às quais teve acesso em decorrência da vistoria realizada nesta data.

Pedro Leopoldo- MG, ... de .....de .....

.....

NOME COMPLETO Cargo Matrícula

ANEXO III

DECLARAÇÃO DE DISPENSA DE VISTORIA TÉCNICA

A empresa .....(nome ou razão social da empresa) ....., CNPJ/MF n.º....., representada por seu Responsável Técnico .....(Nome do responsável) ....., CPF nº ....., Dispensa a visita técnica e DECLARA que tem ciência das condições atuais de infraestrutura de Tecnologia da Informação da Prefeitura Municipal de Pedro Leopoldo e encontra em condições de execução dos serviços objeto da presente contratação, nos termos do Art. 63, § 4º Lei 14.133/2021, bem como das condições de acordo de níveis de serviços para o cumprimento das obrigações a serem contratadas e SE COMPROMETE a prestar fielmente os serviços com a qualidade necessária dentro dos acordo de níveis de serviços, nos termos do Edital do Pregão Eletrônico nº _____/20... e seus Anexos.

Pedro Leopoldo-MG, ... de .....de 20…..

.....

NOME COMPLETO

RG / UF CPF Representante legal da CONTRATADA

ANEXO IV

Item	Descrição	Valor Mensal do Serviço	Valor Total do Serviço (60 Meses)
01	Contratação de empresa especializada em prestação de serviços de segurança da Informação, incluindo equipamentos UTM necessários para prestação dos serviços, monitoramento e suporte especializado em modalidade 24x7, incluindo instalação de equipamentos, configuração, documentação e capacitação de no mínimo 16(dezesseis) horas aos servidores da Divisão de Tecnologia da Informação.	R$ 3.500,00	R$ 210.000,00

ANEXO I DO TERMO DE REFERÊNCIA

SOFTWARE DE SEGURANÇA DA INFORMAÇÃO

ITEM	DESCRIÇÃO	UNIDADE MEDIDA	QUANTIDADE
1.	Contratação de empresa especializada em prestação de serviços de segurança da Informação, incluindo equipamentos UTM necessários para prestação dos serviços, monitoramento e suporte especializado em modalidade 24x7, incluindo instalação de equipamentos, configuração, documentação e capacitação de no mínimo 16 (dezesseis) horas aos servidores da Divisão de Tecnologia da Informação.	Mês	60 meses

ANEXO II DO TERMO DE REFERÊNCIA

DECLARAÇÃO DE VISITA TÉCNICA

Declaramos, para fins de participação no Pregão Eletrônico nº ..... /....., que a empresa ..... (nome ou razão social da empresa) ....., CNPJ/MF n.º....., representada por seu Responsável Técnico..... (nome do responsável) ....., CPF nº....., em visita realizada às instalações da Prefeitura Municipal de Pedro Leopoldo, está ciente das condições atuais de infraestrutura, bem como das quantidades, marcas e configurações dos equipamentos de informática e ainda dos softwares em utilização pela instituição, e que recebeu instruções e informações adicionais necessárias ao atendimento do objeto e demais condições do Edital, não havendo, portanto, nenhuma dúvida que prejudique a apresentação de uma proposta completa e com todos os detalhes.

Declaramos ainda, que a supramencionada empresa está ciente do compromisso assumido de manter sigilo sobre todas as informações às quais teve acesso em decorrência da vistoria realizada nesta data.

Pedro Leopoldo- MG, ... de .....de .....

.....
NOME COMPLETO Cargo Matrícula

ANEXO III DO TERMO DE REFERÊNCIA

DECLARAÇÃO DE DISPENSA DE VISTORIA TÉCNICA

A empresa .....(nome ou razão social da empresa) ....., CNPJ/MF n.º....., representada por seu Responsável Técnico .....(Nome do responsável) ....., CPF nº ....., Dispensa a visita técnica e DECLARA que tem ciência das condições atuais de infraestrutura de Tecnologia da Informação da Prefeitura Municipal de Pedro Leopoldo e encontra em condições de execução dos serviços objeto da presente contratação, nos termos do Art. 63, § 4º Lei 14.133/2021, bem como das condições de acordo de níveis de serviços para o cumprimento das obrigações a serem contratadas e SE COMPROMETE a prestar fielmente os serviços com a qualidade necessária dentro dos acordo de níveis de serviços, nos termos do Edital do Pregão Eletrônico nº _____/20... e seus Anexos.

Pedro Leopoldo-MG, ... de .....de 202...

.....
NOME COMPLETO
RG / UF CPF Representante legal da CONTRATADA

ANEXO IV DO TERMO DE REFERÊNCIA

Item	Descrição	Valor Mensal do Serviço	Valor Total do Serviço (60 Meses)
01	Contratação de empresa especializada em prestação de serviços de segurança da Informação, incluindo equipamentos UTM necessários para prestação dos serviços, monitoramento e suporte especializado em modalidade 24x7, incluindo instalação de equipamentos, configuração, documentação e capacitação de no mínimo 16(dezesseis) horas aos servidores da Divisão de Tecnologia da Informação.	R$	R$

ANEXO II

MINUTA DE CONTRATO ____/2024

Processo Licitatório: 032/2024
Modalidade: Pregão Eletrônico
Número da Licitação: 027/2024
Contratação de Serviço

O Município de Pedro Leopoldo, entidade de direito público interno, com sede no(a) Rua Dr. Cristiano Otoni, 555 - Centro - PEDRO LEOPOLDO - MG, CNPJ/MF 23.456.650/0001-41, neste ato representado pela Sr. Hélder Sebastião Santos - Secretário Municipal de Administração, doravante denominado simplesmente "CONTRATANTE", de um lado; e, de outro lado,_____ , com sede no (a)_____ , neste ato representada pelo seu representante legal Sr.(a), CPF nº, CI nº, doravante denominada simplesmente "CONTRATADA", têm por justo e contratado o que se segue:

CLÁUSULA PRIMEIRA: DO OBJETO

1. Constitui objeto do presente contrato, nos termos do ***Processo Licitatório nº 032/2024 na Modalidade de Pregão Eletrônico nº 027/2024*** adjudicado e homologado em favor da **Contratação de empresa especializada para prestação de serviços de segurança de rede de computadores composta por firewall com funcionalidades UTM (Unified Threat Management) incluindo serviços de suporte especializado, para atender as demandas da Secretaria de Administração, de acordo com o Edital e seus anexos**, nos termos da proposta apresentada, que fica desde já fazendo parte integrante do presente instrumento.

1.1. Requisitos da Contratação

1.1.1. Requisitos técnicos:

1.1.1.2. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.0 Gbps ou superior.

1.1.1.3. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

1.1.1.4. Desempenho mínimo de 3.3 Gbps de IPS.

1.1.1.5. Suporte mínimo de 500.000 conexões simultâneas/concorrentes no modo DPI.

1.1.1.6. Suporte mínimo de 20.000 novas conexões por segundo.

1.1.1.7. Deve suportar expansão de armazenamento interno para até 256Gb.

1.1.1.8. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

1.1.1.9. Deve possuir 16 interfaces 1 GbE padrão RJ-45.

1.1.1.10. Deve possuir 3 interfaces 10GbE SFP+; Deve possuir 1 do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.

1.1.1.11. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

1.1.1.12. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos, com aquisição de licença complementar.

1.1.1.13. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 100 usuários simultâneos, com aquisição de licença complementar.

1.1.1.14. Deve suportar 250 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

1.1.1.15. Deve suportar, no mínimo, 2.1 Gbps de desempenho de VPN IPSEC.

1.1.1.16. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

1.1.1.17. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

1.1.1.18. O Equipamento deverá ser homologado pela ANATEL.

1.1.1.19. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

1.1.1.20. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 12(doze) meses, renováveis de acordo com o prazo da prestação e execução dos serviços.

1.1.1.21. A garantia do hardware deverá ser de 12 (doze) meses.

1.1.1.22. É imprescindível que a solução possua um limite mínimo de tamanho de arquivos de, ao menos, 400Mb, no uso da tecnologia 'gateway antimalware' liveprotection, já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

1.2.Características Gerais Dos Firewalls Físicos

1.2.1.Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

1.2.2.Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

1.2.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

1.2.4. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.

1.2.5. Não serão aceitas soluções baseadas em PCs (personal computers) de uso geral, assim como soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

1.2.6. Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 12(doze) meses, incluindo garantia e suporte, renováveis de acordo com o prazo da prestação e execução dos serviços.

1.3.Características Diversas

1.3.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

1.3.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do túnel IPSec.

1.3.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

1.3.5. Deve possuir proteção anti-spoofing.

1.3.6. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP.

1.3.7. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

1.3.8. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

1.3.9. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

1.3.10. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

1.3.10.1. Latência;

1.3.10.2. Jitter;

1.3.10.3. Perda de pacotes.

1.3.11. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico.

1.3.12. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

1.3.13. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

1.3.14. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

1.3.15. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

1.3.16. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

1.3.17. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

1.3.18. Deve suportar DHCP relay.

1.3.19. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

1.3.20. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.

1.3.21. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares P2P (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

1.3.22. Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

1.3.23. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

1.3.24. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

1.3.25. Detectar e bloquear a origem de portscans.

1.3.26. Deve permitir o bloqueio de ataques.

1.3.27. Deve permitir o bloqueio de exploits conhecidos.

1.3.28. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP.

1.3.29. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação.

1.3.30. Implementar DSCP (Differentiated Services Code Points).

1.3.31. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

1.3.32. Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice Over IP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

1.3.33. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

1.3.34. Possuir suporte ao protocolo SNMP versões 2 e 3.

1.3.35. Possuir suporte a log via syslog.

1.3.36. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

1.3.37. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

1.3.38. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.

1.3.39. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

1.3.40. Para tráfego criptografado SSL/TLS, deve decriptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

1.3.41. Controle, inspeção e decriptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.

1.3.42. Deve permitir a funcionalidade de ARP bridging.

1.3.43. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm".

1.4. **Características De VPN**

1.4.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

1.4.2. Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256

1.4.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

1.4.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

1.4.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

1.4.6. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

1.4.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

1.4.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

1.4.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

1.4.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

1.4.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

1.4.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

1.4.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

1.4.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

1.4.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

1.4.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

1.5. **Alta Disponibilidade**

1.5.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

1.5.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover.

1.5.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

1.5.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

1.5.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

1.5.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

1.5.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

1.5.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

1.5.9. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, RSTP, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

1.6. **Controle De Ameaças**

1.6.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

1.6.2. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

1.6.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

1.6.4. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

1.6.5. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

1.6.6. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

1.6.7. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

1.6.8. Implementar interface CLI segura através do protocolo SSH.

1.6.9. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

1.6.10. A solução deve permitir criar regras de exceção de acordo com a proteção.

1.6.11. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

1.6.12. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

1.6.13. A solução deve ser capaz de proteger contra ataques a DNS.

1.6.14. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

1.6.15. A solução deve ser capaz de prevenir acesso a websites maliciosos.

1.6.16. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

1.6.17. A solução deverá receber atualizações de um serviço baseado em cloud.

1.6.18. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

1.6.19. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

1.6.20. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

1.6.21. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.

1.6.22. A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

1.7. Proteção Contra Ataques Avançados

1.7.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

1.7.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

1.7.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

1.7.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

1.7.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

1.7.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

1.7.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

1.7.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

1.7.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

1.7.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este

1.8. **Características De Filtro De Conteúdo Web**

1.8.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.

1.8.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local.

1.8.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.

1.8.4. Permitir a customização de página de bloqueio.

1.8.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

1.8.6. Deve permitir submissão de novos sites para categorização.

1.8.7. Permitir a classificação dinâmica de sites web, URLs e domínios.

1.8.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

1.8.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

1.8.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

1.9. Características De Autenticação

1.9.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

1.9.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

1.9.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

1.9.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

1.9.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

1.9.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW.

1.9.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

1.9.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

1.9.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

1.9.10. A solução deve possibilitar SSO via API

1.10. Características De Administração

1.10.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

1.10.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

1.10.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

1.10.4. Possuir mecanismo para agendamento realização das cópias de segurança (backups) de configuração.

1.10.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

1.10.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

1.10.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.

1.10.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.

1.10.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

1.10.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.

1.10.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

1.10.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real, estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

1.10.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

1.10.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.

1.10.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

1.10.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

1.10.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

1.10.18. Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

1.10.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

1.10.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

1.10.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

1.10.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

1.10.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

1.10.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

1.10.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

1.10.26. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto-provisionamento da plataforma através de ponto central de gerenciamento.

1.10.27. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações.

1.10.28. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas.

1.10.29. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful.

1.11. **Gerenciamento Unificado e Relatórios**

1.11.1. Deve possuir solução de gerenciamento centralizado em nuvem do mesmo fabricante, para gerenciamento de toda solução.

1.11.2. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções dos usuários da console que determinem usuários

a. Grupos de firewalls permitidos

b. Funcionalidades permitidas por firewall ou grupo de firewalls de acordo com o perfil de uso designado

c. Perfil de nível de acesso (escrita, leitura, administração, relatórios)

1.11.3. Deve suportar organizar os dispositivos administrados em grupos. Estes grupos devem permitir isolamento tanto de acesso para os administradores como de configuração massiva ou individual

1.11.4. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls.

1.11.5. Deve apresentar estado dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

1.11.6. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

1.11.7. O gerenciamento deve permitir/possuir:

a. Criação e administração de políticas de firewall e controle de aplicação

b. Monitoração de logs;

c. Investigação de evendos de segurança e falhas (debugging)

d. Acesso concorrente de administradores, conforme políticas e perfis previamente definidos

1.11.8. Deve permitir o provisionamento e configuração sem intervenção de operadores (Zero-Touch). Os firewalls devem se conectar automaticamente à plataforema de gerencia, e à partir desta conexão receberem as configurações previamente determinadas pelos operadores da plataforma.

1.11.9. A solução de gerenciamento deve ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL

1.11.10. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

1.11.11. A solução deve possuir tela situacional com todo os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador:

a. nome do firewall

b. número de série

c. modelo

d. versão do firmware e estado da conectividade do equipamento com a gerência em online ou offline.

1.11.12. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;

1.11.13. Deve centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento, possibilitando comparação de configurações que evitem sobreposição de regras e conflitos de configuração.

1.11.14. A solução deve possuir Dashboard com sumario de alertas e informação de status de licença

1.11.15. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo

1.11.16. Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência

1.11.17. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN

1.11.18. A solução deve permitir a criação de modelos de configuração (templates) para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls

1.11.19. A solução deve possibilitar a geração de templates de configuração à partir da configuração vigente em um firewall selecionado pelo administrador da plataforma, e possibilitar que este template possa ser editado e utilizado em outros firewalls gerenciados pela plataforma.

1.11.20. Os modelos de configuração (templates) devem suportar configurações de interfaces físicas ou virtuais

1.11.21. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

1.11.22. Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas.

1.11.23. De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento;

1.11.24. Deve incluir console de configuração e monitoramento SD-WAN, possibilitar a criação de políticas SD-WAN em todos os elementos gerenciados, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

1.11.25. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

1.11.26. Durante a alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

1.11.27. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, este processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente

1.11.28. A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.

1.11.29. A solução deve oferecer monitor de auditoria de configuações aplicadas aos firewalls gerenciados pela plataforma, permitindo comparativo diferencial entre registros para rápida identificação de configurações e alterações aplicadas.

1.11.30. A solução deve oferecer módulo centralizado que possibilite realização e armazenamento de backup de configurações dos firewalls gerenciados.

1.11.31. A solução deve oferecer possibilidade de auditoria de configurações.

1.11.32. A solução deve possibilitar o monitoramento em tempo real dos firewalls gerenciados, informando minimamente:

a. Utilização de CPU/Processamento
b. Aplicações em uso e seu consumo de banda
c. Interfaces em uso e utilizaçào de banda
d. Conexões concorrentes em uso

1.11.33. A solução deverá permitir visualizar sumario com as informações referentes as principais ameaças protegidas pelos firewalls

1.11.34. Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a geração de relatórios e monitoramento em tempo real.

1.11.35. A solução deverá prover relatórios com no mínimo histórico de 365 dias

1.11.36. A solução deverá prover relatórios referente as atividades dos usuários

1.11.37. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações:

a. nome da aplicação
b. quantidade de conexões
c. percentual que a aplicação representa do tráfego da rede e quantidade de Megabytes trafegados

1.11.38. A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações:

a. nome do usuário
b. quantidade de conexões
c. percentual que tráfego do usuário representa na rede
d. quantidade de Megabytes trafegados

1.11.39. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações:

a. endereço IP
b. quantidade de conexões
c. percentual que tráfego que o IP representa na rede
d. quantidade de Megabytes trafegados

1.11.40. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede

1.11.41. A solução deverá arquivar relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF

1.11.42. A solução deverá permitir geração e envio agendado de relatórios

1.11.43. A solução deve permitir a customização de alertas e notificações, possibilitando o envio de e-Mail com as informações relativas a este evento.

1.11.44. A solução deve possibilitar configuração e monitoramento centralizados de VPNs entre os firewalls gerenciado

1.11.45. A solução deve apresentar consoles de indicação com os principais eventos, riscos e ameaças contendo:

a. Aplicações de maior risco, e volume de dados consumido por estas
b. Aplicações de maior utilização, por volume de dados transferidos e conexões consumidas
c. Aplicações de maior utilização, por categoria

1.11.46. A solução deve apresentar consoles de indicação dos principais usuários contendo:

a. Usuários utilizando mais conexões

b. Usuários consumindo mais dados

1.11.47. A solução deve apresentar console de indicação de:
- a. Virus/Spyware blockeados
- b. Intrusões bloqueadas
- c. Botnets bloqueados
- d. Origens e destinos mais utilizados

1.11.48. A solução deve apresentar console de indicação de Aplicações indicando:
- a. Aplicações identificadas
- b. Categorização e uso das aplicações
- c. Risco das aplicações

1.11.49. A solução deve permitir visualização de eventos correlacionados que possam ser investigados por:
- a. Lista de eventos correlacionados com opção de navegação "drilldown"; ou
- b. Modo gráfico; ou
- c. Lista de logs

1.11.50. A solução deve apresentar console de monitoramento de produtividade dos usuários, indicando suas características de navegação de acordo com políticas previamente estabelecidas e categorizadas como:
- a. Produtivas
- b. Não produtivas
- c. Aceitáveis para a política de uso corporativa
- d. Inaceitáveis para a política de uso corporativa
- e. Customizadas

1.11.51. A solução deve permitir visualização de topologia do firewal e elementos a ele conectados (dispositivos de rede complementares, dispositivos de usuários, Access Points)

1.11.52. O Fabricante deverá comprovar que possui tecnologia holística capaz de integrar suas principais soluções em uma base centralizada gráfica com informações e alertas, comprovando integração de pelo menos 2 de suas plataformas de segurança.

1.12. **Treinamento de Capacitação:**

1.12.1.Deverá ser realizado um treinamento para solução integrada de Firewall e Service Gateway a ser utilizada na prestação dos serviços, ministrado por profissional certificado na solução. Este será realizado na Prefeitura para até 8 (oito) pessoas em uma única turma. A duração deverá ser de no mínimo 16 (dezesseis) horas, abordando as os seguintes tópicos:

- Introdução à plataforma e funcionalidades do equipamento;
- Introdução ao software de gerenciamento;
- Introdução à interface gráfica de usuário;
- Regras de Firewall;
- Zonas de segurança;
- Políticas de segurança;
- Autenticação de usuários;
- Proteção de rede;
- NAT (Network Addres Translation).

1.12.2.O treinamento deve ser vinculado as plataformas vencedoras do item 1;

1.12.3.Qualquer despesa incorrida tais como escopo do serviço, passagens aéreas, locação de veículos, hospedagens e alimentação do instrutor será de responsabilidade exclusiva do contratado.

1.12.4.Será de responsabilidade da Prefeitura a disponibilização de infraestrutura e dos equipamentos para montagem da sala de aula e laboratório.

1.12.5.Os treinamentos serão ministrados no idioma português. Os materiais fornecidos podem estar no idioma português ou inglês.

1.12.6.Após a realização do treinamento, deverá ser fornecido um certificado formal de participação para cada participante do evento.

1.12.7.A proponente vencedora deverá apresentar, durante a sessão do pregão, catálogo ou manual impresso publicado pelo fabricante do equipamento ofertado, em língua portuguesa ou inglesa, com identificação precisa da página onde se encontram as informações sobre o atendimento de cada requisito exigido na especificação técnica;

1.12.8.Poderá ser aceita cópia de documento publicado no sítio do fabricante na Internet que comprove as especificações do equipamento, desde que da mesma conste o endereço eletrônico de acesso irrestrito, devendo estar disponível para acesso ao público em geral e passível de verificação durante a sessão do pregão.

1.12.9.Todas as declarações deverão ser apresentadas com firma reconhecida em cartório e acompanhadas dos documentos que comprovem a capacidade legal de quem as assinou;

1.12.10.Todos os documentos deverão estar vigentes no dia previsto para realização deste pregão.

1.13. Do Suporte, Garantia e Assistência Técnica:

1.13.1. Todos os serviços de suporte e manutenção preventiva ou corretiva, assim como a substituição de peças e suprimentos necessários ao perfeito funcionamento do bem durante a vigência do contrato, serão prestados pelo fornecedor.

1.13.2. O suporte técnico será realizado remoto ou “on-site”, de acordo com a necessidade e requisição da Prefeitura, sem ônus adicional durante a vigência do contrato.

1.13..3. A Contratada deverá disponibilizar um aplicativo via web para abertura de chamados de suporte técnico, ou Central de Atendimento ou correio eletrônico do prestador de serviços;

1.13.4. O prazo de atendimento para solução deverá ser respeitado de acordo com a tabela de prioridades e prazos abaixo:

Serviços	**Prioridade***	**Prazo**

Atendimento Telefônico Abertura de Chamados WEB	**1,2 e 3**	24x7 (24 Horas / 7 Dias Semana)
Horário de Atendimento	**1,2 e 3**	24x7 (24 Horas / 7 Dias Semana)
Tempo de Resposta para Serviços Remotos	**2**	Até 2 Horas Úteis
	3	Até 4 Horas Úteis
Atendimentos “On Site”	**1**	Até 4 Horas Úteis

(*) Descrição das Prioridades:

1 - Não conformidades que restringem completamente (80 a 100%) o funcionamento de todo o sistema ou apresentem-se como ameaças concretas. *Ex.:* Paralisação do Firewall ou da rede WAN.

2 - Não conformidades que restringem parcialmente (26 a 80%) o funcionamento de todo o sistema ou apresentam-se como vulnerabilidades para possíveis ameaças. *Ex.:* Lentidão na performance

3 - Não conformidades que não restringem (0 a 25%) o funcionamento de todo o sistema, mas sim de usuários isolados *Ex.:* Um usuário bloqueado

Parágrafo único: Incluídos no(s) preço(s) unitário(s) estão todos os impostos, taxas e encargos sociais, obrigações trabalhistas, previdenciárias, fiscais e comerciais, assim como despesas com transportes, os quais correrão por conta do fornecedor.

CLÁUSULA SEGUNDA: DA VIGÊNCIA

2.1. O prazo de vigência da contratação é de 60 (sessenta) meses, contados da data de assinatura do Contrato, prorrogável por até 15 anos , conforme artigo 106 e 114 da Lei nº 14.133, de 2021.

CLÁUSULA TERCEIRA : EXECUÇÃO CONTRATUAL

3.1. O prazo de entrega e início da prestação dos serviços (incluindo instalação, configuração do equipamento e capacitação da solução entregue), se dará em até 60 (sessenta) dias corridos, contados a partir do recebimento pelo fornecedor da Ordem de serviços

3.2. A CONTRATADA deverá informar à CONTRATANTE, quando da entrega dos equipamentos com, no mínimo, 10 (dez) dias corridos de antecedência, ficando a CONTRATADA responsável pelo transporte e entrega de equipamentos e/ou partes componentes da solução integrada de segurança da informação.

3.3. A Ordem de serviço ou de fornecimento de bens indicará a quantidade, os endereços de entrega e da instalação e nome do responsável pelo recebimento, acompanhado de e-mail e/ou telefone para contato.

3.4. A montagem e a instalação dos equipamentos deverão ser feitas pelo fornecedor, não sendo aceito a terceirização dos serviços no local de entrega e em horários a serem agendados pela Divisão de Tecnologia da Informação da Prefeitura, na sede da Prefeitura Municipal de Pedro Leopoldo, localizada à Rua Dr Cristiano Otoni, 555, Centro.

3.5. Não será permitida a subcontratação do objeto dessa contratação

3 .6. A assistência técnica e suporte deverão ser prestados por profissionais especializados, com certificados devidamente emitidos, com experiência nos serviços e produtos que compõem a solução, assim como recursos ferramentais necessários, disponibilizados pela CONTRATADA, para a prestação dos serviços.

3.7. Mediante termo aditivo, e de acordo com a capacidade operacional do CONTRATADO, o CONTRATANTE poderá, nos termos da Lei Federal nº 14.133/21 e considerando suas necessidades, fazer acréscimos ou supressões nos valores limites desse contrato, durante o período de sua vigência, incluídas as prorrogações, por meio de solicitação justificada do Secretário Municipal de Administração ou outra autoridade competente.

CLÁUSULA QUARTA: DAS OBRIGAÇÕES DO CONTRATANTE

4.1. Prestar à Contratada todas as informações solicitadas e necessárias para o fornecimento do bem;

4.2. Designar servidores para acompanhar e fiscalizar a execução do instrumento;

4.3. Entregar/enviar a Ordem de Compra à Contratada;

4.4. Exigir o cumprimento de todos os compromissos assumidos pela Contratada, nos termos do edital e da proposta;

4.5. Notificar a Contratada, por escrito, a ocorrência de eventuais falhas ou imperfeições no fornecimento do bem, fixando prazo para sua correção;

4.6. Aplicar à Contratada as sanções motivadas pela inexecução total ou parcial do objeto;

4.7. Cientificar o NUPAD - Núcleo de Procedimento para Apuração de Descumprimento de Cláusulas Contratuais (NUPAD), no endereço eletrônico nupad@pedroleopoldo.mg.gov.br, para adoção das medidas cabíveis quando do descumprimento de obrigações pela Contratada;

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

CLÁUSULA QUINTA : DAS OBRIGAÇÕES DA CONTRATADA

5.1. Preparar e dotar de infraestrutura logística como contratação de software, link, pessoal de apoio, veículo, combustível, telefone e diárias para operacionalização dos serviços.

5.2. Cumprir rigorosamente todas as exigências estabelecidas neste Termo de Referência;

5.3. Realizar os serviços de acordo com as especificações;

5.4. Providenciar a imediata correção das irregularidades apontadas pela secretaria solicitante;

10.5. Garantir a boa qualidade dos serviços prestados, bem como o bom andamento dos jogos.

5.6. Responsabilizar-se por todos e quaisquer danos e/ou prejuízos que vierem causar à Secretaria solicitante ou a terceiros;

5.7. Comunicar ao município, no prazo de 24 horas, qualquer ocorrência anormal que impossibilite o cumprimento das obrigações assumidas.

5.8. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, garantindo sigilo e inviolabilidade das informações, respeitando as hipóteses constitucionais e legais de quebra de sigilo.

5.9. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Administração.

5.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

5.11. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

CLÁUSULA SEXTA: DO PAGAMENTO

6.1. A Prefeitura Municipal de Pedro Leopoldo promoverá o pagamento no prazo de 28 (vinte e oito) dias contados do recebimento da Nota Fiscal, devidamente certificada pela Secretaria solicitante.

6.2. As Notas Fiscais ou documentos que a acompanharem para fins de pagamento que apresentarem incorreções serão devolvidos à CONTRATADA e o prazo para o pagamento passará a correr a partir da data da reapresentação dos documentos, considerados válidos pelo CONTRATANTE.

6.3. É vedado à Contratada transferir a terceiros os direitos ou créditos decorrentes do contrato ou instrumento equivalente.

6.4. Nas Notas Fiscais deverão vir os dados bancários completos da CONTRATADA, sob pena de não realização do pagamento até a informação dos mesmos, de obrigação da CONTRATADA.

6.5. Para que os pagamentos possam ser efetuados, a contratada deverá apresentar, junto à nota fiscal de produtos, a seguinte documentação:

I - Documentos comprobatórios da regularidade fiscal e regularidade trabalhista;

6.6. Para que os pagamentos possam ser efetuados, a contratada deverá apresentar, junto a nota fiscal, os documentos comprobatórios da regularidade fiscal e regularidade trabalhista;

6.7.Sobre o valor devido ao contratado, a Administração efetuará as retenções tributárias cabíveis;

6.8. Quanto ao Imposto sobre Serviços de Qualquer Natureza (ISSQN), será observado o disposto na Lei Complementar Nº 116, de 2003, e legislação municipal aplicável.

7. DOS CRITÉRIOS DE ATUALIZAÇÃO FINANCEIRA

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de 01 (um) ano contado da data do orçamento estimado para a presente contratação.

7.2. Após o interregno de 01 (um) ano, os preços iniciais serão reajustados, mediante a aplicação do Índice Nacional de Preços ao Consumidor Amplo – IPCA ou outro que houve por substituí-lo, caso mais favorável à Administração Pública, como critério de atualização monetária, nos termos do art. 25, §7º, da Lei nº 14.133/2021

7.3. A data-base estará vinculada à data do orçamento estimado e adjudicado ao licitante vencedor.

7.4. A extinção do contrato não configurará óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

7.5. O pedido de restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação, nos termos do art. 107 e 131, parágrafo único, da Lei nº 14.133/2021.
7.6. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

7.7. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

7.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente.

7.9. O Contrato poderá ser rescindido nas hipóteses arroladas nos artigos 137 e 138 da Lei Federal nº 14.133/2021.

CLÁUSULA OITAVA: DOS RECURSOS ORÇAMENTÁRIOS

8.1. As despesas com execução do presente contrato, correrão por conta da seguinte dotação do orçamento vigente:

132 - 02.05.05.04.126.0011.2039.3.3.90.40.00 - 5001.500.000 - RECURSOS NÃO VINCULADOS DE IMPOSTOS - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PESSOA JURÍDICA.

8.2. O custo total máximo estimado para a aquisição do objeto ora licitado é de R$_____, conforme ficha aprovada na Lei orçamentária do Exercício.

CLÁUSULA NONA: DA GESTÃO DO CONTRATO E FISCALIZAÇÃO

9.1.O contrato ou instrumento equivalente deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

9.2. A execução do contrato ou instrumento equivalente deverá ser acompanhada e fiscalizada pelo(s) fiscal(is), ou pelos respectivos substitutos.

9.3. O contrato ou instrumento equivalente oriundo desta contratação terá como responsáveis:

9.3.1. GESTOR:

a) Hélder Sebastião dos Santos - Secretário Municipal de Administração;

9.3.2. FISCAIS:

a) Alexandre Thadeu Clemenete Bassouto - Analista de Sistemas e Redes III - Fiscal Técnico - Titular
b) Paula Poliana Gonçalves Braga- Assistente Administrativo II - Fiscal Administrativo - Titular
c) Victor Hugo Pereira Reis - Gerente de Tecnologia da Informação - Fiscal Administrativo/Técnico - Substituto Titular

9.3.2.1. O fiscal do contrato ou instrumento equivalente anotará em registro próprio todas as ocorrências relacionadas à execução, determinando o que for necessário para a regularização das faltas ou dos defeitos observados.

9.3.2.2. O(s) fiscal(is) do contrato ou instrumento equivalente informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência.

9.4. O contratado será obrigado a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato ou instrumento equivalente em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados.

9.5. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato ou instrumento equivalente, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante.

9.6. Somente o contratado será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato ou instrumento equivalente.

9.6.1. A inadimplência do contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato ou instrumento equivalente.

9.7. As comunicações entre a Administração e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, excepcionalmente, o uso de mensagem eletrônica para esse fim.

9.8. Antes do pagamento da nota fiscal ou da fatura, deverá ser consultada pela Secretaria Municipal de Administração do Município, a situação da empresa junto ao Cadastro de Fornecedores do Município – CFM.

9.8.1. Serão exigidos a Certidão Negativa de Débito (CND) relativa a Créditos Tributários Federais e à Dívida Ativa da União, o Certificado de Regularidade do FGTS (CRF), a Certidão Negativa de Débito Municipal e a Certidão Negativa de Débitos Trabalhistas (CNDT), caso esses documentos não estejam regularizados no CFM.

CLÁUSULA DÉCIMA: DAS SANÇÕES ADMINISTRATIVAS

10.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

10.1.1. 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;

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

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

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

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

10.1.2.4. deixar de apresentar amostra;

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

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

10.1.3.1. recusar-se, sem justificativa, a assinar o contrato, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

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

10.1.5.fraudar a licitação;

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

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

10.1.6.3. induzir deliberadamente a erro no julgamento;

10.1.6.4. apresentar amostra falsificada ou deteriorada;

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

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

10.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos fornecedor as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

10.2.1. advertência;

10.2.2.multa;

10.2.3. impedimento de licitar e contratar e

10.2.4. 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.

10.3. Na aplicação das sanções serão considerados:

10.3.1. a natureza e a gravidade da infração cometida.

10.3.2. as peculiaridades do caso concreto

10.3.3. as circunstâncias agravantes ou atenuantes.

10.3.4. os danos que dela provierem para a Administração Pública.

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

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

10.4.1. Para as infrações previstas nos itens 10.1.1, 10.1.2. e 10.1.3, a multa será de 0,5% a 15% do valor do contrato licitado;

10.4.2. Para as infrações previstas nos itens 10.1.4, 10.1.5, 10.1.6., 10.1.7 e 10.1.8, a multa será de 15% a 30% do valor contrato licitado;

10.4.3. O valor da multa deverá observar o disposto no Art. 156, §1º da Lei 14.133/2021;

10.4.4. Conforme disposto no art.156 § 3º o percentual da multa aplicada nas infrações administrativas previstas no art. 155 seguirão a discricionariedade do gestor na fixação de multa, sendo os percentuais sugeridos meramente indicativos;

10.5. 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;

10.6. 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;

10.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 10.1.1, 10.1.2 e 10.1.3, 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, conforme estabelece o art.156,§ 4º;

10.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 16.1.4, 16.1.5, 16.1.6, 16.1.7 e 16.1.8, bem como pelas infrações administrativas previstas nos itens 16.1.1, 16.1.2 e 16.1.3 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;

10.9. A recusa injustificada do fornecedor em assinar o contrato, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item , 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;

10.10. 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, conforme preceitua o art. 158, § 8º;

10.11. 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, 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;

10.12. 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;

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

10.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados, conforme estabelece o art.156, §9º.

CLÁUSULA DÉCIMA PRIMEIRA: DA RESCISÃO

11.1. O presente contrato poderá ser rescindido nas hipóteses arroladas nos artigos 137 e 138 da Lei Federal nº 14.133/2021.

CLÁUSULA DÉCIMA SEGUNDA: DA PUBLICAÇÃO

12.1. Incumbirá ao Município divulgar o presente instrumento no Portal Nacional de Contratações Públicas - PNCP, na forma prevista no art. 94, da Lei Federal nº 14.133/21, bem como no respectivo sítio oficial na Internet , em atenção ao art. 91, caput, da Lei Federal nº 14.133/21.

CLÁUSULA DÉCIMA TERCEIRA: DAS DISPOSIÇÕES GERAIS

13.1. As normas constantes do Edital do certame licitatório integram o presente contrato, independente de transcrição e serão observadas pelas partes.

CLÁUSULA DÉCIMA QUARTA: DO FORO

14.1. Fica eleito o foro da Comarca de Pedro Leopoldo, Estado de Minas Gerais, para dirimir os litígios que decorrem da execução deste instrumento que não puderem ser compostos pela conciliação, conforme art. 92. §1º, da Lei Federal nº14.133/21.

14.2. O presente instrumento é abaixo assinado e entra em vigor, nesta data.

Pedro Leopoldo __ de _____ de 2024.

_____
Hélder Sebastião Santos
Secretário Municipal de Administração

_____
Contratada