CÂMARA MUNICIPAL DE ITABIRITO

PREGÃO ELETRÔNICO

11/2024

CONTRATANTE (UASG)

CÂMARA MUNICIPAL DE ITABIRITO (UASG 930.116)

OBJETO

Contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall e access point, para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara de Itabirito

VALOR TOTAL DA CONTRATAÇÃO

R$ 195.487,27 (cento e noventa e cinco mil, quatrocentos e oitenta e sete reais e vinte e sete centavos)

DATA DA SESSÃO PÚBLICA

Dia **06/02/2024** às **13hs (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

menor preço por lote

MODO DE DISPUTA:

aberto

PREFERÊNCIA ME/EPP/EQUIPARADAS

sim

EDITAL

CÂMARA MUNICIPAL DE ITABIRITO/MG (UASG 930.116)

PREGÃO ELETRÔNICO Nº 11/2024

PROCESSO ADMINISTRATIVO Nº 465/2024

Torna-se público que a CÂMARA MUNICIPAL DE ITABIRITO, por meio do Setor de Licitações e Contratos, sediado na Av. Queiroz Junior, nº 639, bairro Praia, Itabirito/MG, CEP 35.450-228, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto Municipal nº 14.754, de 10 de fevereiro de 2023, e demais legislações aplicáveis e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall e access point, para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara de Itabirito. Conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2 A licitação será realizada em 2 lotes, formado por 06 (seis) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

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

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

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

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

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

2.5. Não poderão disputar esta licitação:

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

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

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

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

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

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

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

2.5.8. agente público do órgão ou entidade licitante;

2.5.9. *pessoas jurídicas reunidas em consórcio;*

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

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

2.6. O impedimento de que trata o item 2.5.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

2.7. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.5.2 e 2.5.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

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

2.9. O disposto nos itens 2.5.2 e 2.5.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

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

2.11. A vedação de que trata o item 2.5.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.12.1 deste Edital.

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

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

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

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

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

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

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

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

3.7. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

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

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

3.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

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

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

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

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

3.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

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

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

4. DO PREENCHIMENTO DA PROPOSTA

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

4.1.1. valor unitário e total do item;

4.1.2. Marca e fabricante, se for o caso;

4.1.3. Quantidade cotada, onde o licitante NÃO poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação;

4.1.4. Descrição do objeto, atendendo à especificação do Termo de Referência;

4.1.5. Dados Bancários para pagamento;

4.1.6. prazo de validade da proposta não inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

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

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.7.1. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

4.7.2. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no item 4.9.

4.8. Em se tratando de serviços com fornecimento de mão de obra em regime de dedicação exclusiva, o licitante deverá indicar os sindicatos, acordos coletivos, convenções coletivas ou sentenças normativas que regem as categorias profissionais que executarão o serviço e as respectivas datas bases e vigências, com base na Classificação Brasileira de Ocupações – CBO.

4.9. Em todo caso, deverá ser garantido o pagamento do salário normativo previsto no instrumento coletivo aplicável ou do salário-mínimo vigente, o que for maior.

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

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

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

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

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

5.5. O lance deverá ser ofertado pelo valor unitário do item;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

5.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser *de R$ 10,00 (dez reais).*

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

5.10. O procedimento seguirá de acordo com o modo de disputa adotado.

5.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

5.11.1. A etapa de lances da sessão pública terá duração de 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.

5.11.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.11.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.11.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

5.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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

5.12.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

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

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

5.13. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “fechado e aberto”, poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

5.13.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 5.13, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

5.13.2. A etapa de lances da sessão pública terá duração de 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.

5.13.3. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.13.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.13.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.13.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

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

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

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

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

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

5.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.20.1. 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.

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

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

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

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

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

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

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;

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

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

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;

empresas brasileiras;

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

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

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

5.22.1. Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo.

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

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

5.22.4. O pregoeiro concederá o prazo de até 30 minutos, prorrogável por igual período, para envio da negociação.

5.22.4.1. decorrido o prazo informado no item anterior, em caso de ausência de resposta da negociação, o pregoeiro poderá proceder com a desclassificação da proposta do primeiro colocado em caso da mesma se encontrar acima do valor estimado.

5.22.4.2. decorrido o prazo informado, em caso de ausência de resposta da negociação, o pregoeiro procederá com a classificação da proposta do primeiro colocado em caso da mesma se encontrar dentro do valor estimado.

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

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

5.22.7. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

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

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.5 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis);

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep); e

6.1.4. Consulta Consolidada de Pessoa Jurídica, mantido pelo Tribunal de Contas da União – TCU (https://www.certidoes-apf.apps.tcu.gov.br/).

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

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

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

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

6.3.3. Constatada a existência de sanção, o licitante será afastado, por falta de condição de participação.

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

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens **Erro! Fonte de referência não encontrada.** e 3.6 deste edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.7.4. apresentar preços unitários acima dos previstos no orçamento da administração;

6.7.5. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.7.6. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 70% (setenta por cento) da média dos demais preços, conforme art. 47, § 3º, II do Decreto Municipal 14.754/2023.

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

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

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

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

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

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

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

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

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

6.11. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

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

6.11.2. Em se tratando de serviços com fornecimento de mão de obra em regime de dedicação exclusiva cuja produtividade seja mensurável e indicada pela Administração, o licitante deverá indicar a produtividade adotada e a quantidade de pessoal que será alocado na execução contratual.

6.11.3. Caso a produtividade for diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

6.11.4. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

6.11.5. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

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

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

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

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

6.14. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

6.15. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

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

6.17. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

6.18. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

7. DA FASE DE HABILITAÇÃO

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

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

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

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

7.4. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

7.5. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia autenticada ou por qualquer outro meio digital que possa ter sua autenticidade conferida.

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

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

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

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

7.10.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

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

7.11.1. A não observância do disposto no item anterior poderá ensejar inabilitação.

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

7.12.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de **02 (duas) horas**, prorrogável por igual período, contado da solicitação do pregoeiro.

7.12.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto.

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

7.13.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.13.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

7.14. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência[1], para:

[1] Art. 64 da lei nº 14.133/2021

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

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

7.14.3. apresentação de documentos de cunho declaratório emitidos unilateralmente pelo licitante.

7.15. A realização ou não de diligência ocorrerá mediante decisão fundamentada do Pregoeiro, caso o mesmo julgue necessário, não se configurando direito subjetivo do licitante a juntada de documentos após o encerramento do prazo estabelecido.

7.16. A apresentação de documentos complementares, substitutivos ou esclarecedores por meio de diligência será realizada nos termos do item 8.15 e findo o prazo concedido sem o envio da nova documentação restará preclusa, em caráter definitivo, a possibilidade de o licitante juntar novos documentos, o que implicará na sua inabilitação ou desclassificação do certame.

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

7.18. Para fins de análise da habilitação quanto ao cumprimento das documentações técnicas e/ou econômico-financeira, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto, independentemente de o profissional pertencer a equipe de apoio.

7.19. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.12.1.

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

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

7.22. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

8. DOS RECURSOS

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

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

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

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.2. o prazo para a manifestação da intenção de recorrer será de 30 (trinta) minutos.

8.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.3.4. na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

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

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

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

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

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

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

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico **www.gov.br/compras.**

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1- O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

a) dar causa à inexecução parcial do contrato;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

b) dar causa à inexecução parcial do contrato que cause grave dano à administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) dar causa à inexecução total do contrato;

d) deixar de entregar a documentação exigida;

e) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

g) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

h) apresentar declaração ou documentação falsa ou prestar declaração falsa durante a licitação ou a execução do contrato;

i) fraudar a licitação ou praticar ato fraudulento na execução do contrato;

j) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

k) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

l) praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, de 1º de agosto de 2013.

9.1.1- Constituem comportamentos que serão enquadrados na letra d, do item 11.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou da execução contratual:

a) deixar de entregar documentação exigida no instrumento convocatório;

b) entregar documentação em manifesta desconformidade com as exigências do instrumento convocatório;

c) fazer entrega parcial de documentação exigida no instrumento convocatório;

d) deixar de entregar documentação complementar exigida pelo Agente de contratação ou Pregoeiro, necessária para a comprovação de veracidade e/ou autenticidade de documentação exigida no edital de licitação.

e) deixar de atender a convocações do Agente de Contratação ou pregoeiro durante o trâmite do certame ou atendê-las de forma insatisfatória.

9.1.2- Constituem comportamentos que serão enquadrados na letra e do item 11.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou da execução contratual:

a) não enviar a proposta adequado ao último lance ofertado ou após a negociação;

b) deixar de encaminhar ou encaminhar em manifesta desconformidade com o instrumento convocatório as amostras solicitadas pelo Agente de Contratação ou Pregoeiro;

c) ofertar preço inexequível na formulação da proposta inicial ou na fase de lances;

d) recusar-se a enviar o detalhamento da proposta quando exigível;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

e) solicitar a desclassificação após a abertura da sessão do certame;

f) abandonar o certame.

9.1.3- Constituem comportamentos que serão enquadrados na letra f do item 11.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou execução contratual:

a) recursar-se a assinar o contrato ou a ata de registro de preço;

b) recusar-se a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração.

9.1.4- Constituem comportamentos que serão enquadrados na letra j do item 11.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou execução contratual, a prática de quaisquer atos direcionados a prejudicar o bom andamento do certame ou do contrato, em especial:

a) agir em concluiu ou em desconformidade com a lei;

b) induzir deliberadamente a erro no julgamento;

c) apresentar amostra falsificada ou deteriorada.

9.2- O licitante ou contratado que incorra nas infrações previstas, garantido o contraditório e a ampla defesa, sujeitar-se-ão às seguintes sanções:

a) advertência;

b) multa;

c) impedimento de licitar e contratar;

d) declaração de inidoneidade para licitar ou contratar.

9.2.1- A aplicação das sanções acima previstas não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

9.2.2- A sanção de **advertência** será aplicável nas hipóteses de inexecução parcial do contrato que não implique em prejuízo ou dano à administração, bem como na hipótese de descumprimento de pequena relevância praticado pelo licitante ou fornecedor e que não justifique imposição de penalidade mais grave.

9.2.3- A sanção de **multa** terá natureza moratória ou compensatória e poderá ser aplicada isolada ou cumulativamente com as demais sanções acima previstas, no caso de cometimento de qualquer das infrações administrativas previstas no item 11.1.

9.2.3.1- A multa moratória será aplicada nas hipóteses de atraso injustificado na execução do contrato.

9.2.3.2- A multa compensatória será aplicada nas hipóteses de descumprimento de obrigações contratuais, sendo estabelecidas em razão do grau de importância da obrigação desatendida, objetivando-se a compensação das eventuais perdas nas quais a Administração tenha incorrido.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

.2.3.3- A multa moratória será de 0,5% (cinco décimos por cento) por dia de atraso na entrega de material ou execução do serviço, recaindo o cálculo sobre o valor da parcela inadimplida até o limite de 30% (trinta por cento) do contrato ou do instrumento equivalente.

9.2.3.4- A aplicação de multa de mora não impedirá que a administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções acima previstas.

9.2.3.5- Poderá ser aplicada multa compensatória de até 3% (três por cento) sobre o valor de referência ao licitante ou contratado que retardar o procedimento de contratação, descumprir preceito normativo ou obrigações assumidas, tais como:

a) tumultuar a sessão pública da licitação;

b) propor recursos manifestamente protelatórios em sede de contratação direta ou de licitação;

c) deixar de providenciar o cadastramento da empresa vencedora da licitação ou da contratação direta junto ao Sistema de Cadastro de Fornecedores dentro do prazo concedido, salvo por motivo justificado e aceito pela administração;

d) deixar de cumprir as exigências de reserva de cargos previstas em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz;

e) deixar de cumprir o modelo de gestão do contrato;

f) deixar de complementar o valor da garantia recolhida após solicitação do contratante;

g) não devolver os valores pagos indevidamente pelo contratante;

h) não manter, durante a execução do contrato, todas as condições exigidas para a habilitação, em caso de licitação, ou para a qualificação, em caso de contratação direta, ou, ainda, quaisquer outras obrigações;

i) deixar de regularizar, no prazo definido pela administração, os documentos exigidos pela legislação para fins de liquidação e pagamento da despesa;

j) manter funcionário sem qualificação para a execução do objeto;

k) utilizar as dependências do contratante para fins diversos do objeto do contrato;

l) deixar de substituir empregado cujo comportamento for incompatível com o interesse público, em especial quando solicitado pela administração;

m) deixar de efetuar o pagamento de salários, vale-transporte, vale-refeição, seguros, encargos fiscais e sociais, bem como deixar de arcar com quaisquer outras despesas relacionadas à execução do contrato nas datas avençadas;

n) deixar de apresentar, quando solicitado, documentação fiscal, trabalhista e previdenciária regularizada;

o) deixar de regularizar os documentos fiscais no prazo concedido na hipótese de o licitante ou contratado enquadrar-se como Microempresa, Empresa de Pequeno Porte ou

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

equiparados, nos termos da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;

p) não manter atualizado e-mail para contato, sobretudo dos prepostos, nem informar à gestão e à fiscalização do contrato, no prazo de dois dias úteis, a alteração de endereços, sobretudo quando este ato frustrar a regular notificação de instauração de processo sancionador;

q) subcontratar o objeto ou a execução de serviços em percentual superior ao permitido no edital ou contrato, ou de forma que configure inexistência de condições reais de prestação do serviço ou fornecimento do bem.

9.2.3.6- Poderá ser aplicada multa compensatória de até 5% (cinco por cento) sobre o valor da parcela inadimplida ao licitante ou contratado que entregar o objeto contratual em desacordo com as especificações, condições e qualidade contratadas ou com irregularidades ou defeitos ocultos que o tornem impróprio para o fim a que se destina.

9.2.3.7- Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela administração ao contratado, além da perda desse valor, a diferença poderá ser paga diretamente à administração, descontada da garantia prestada ou cobrada judicialmente.

9.2.3.8- A multa inadimplida poderá ser descontada de pagamento eventualmente devido pela contratante decorrente de outros contratos firmados com a administração municipal.

9.2.4- A sanção de **impedimento de licitar e contratar** com a Administração Pública Municipal será aplicada pelo prazo máximo de três anos, quando não se justificar a imposição de penalidade mais grave, observando-se os parâmetros estabelecidos, aos responsáveis pelas seguintes infrações:

a) dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo: impedimento pelo período de até dois anos;

b) dar causa à inexecução total do contrato: impedimento pelo período de até três anos;

c) deixar de entregar a documentação exigida para o certame: impedimento pelo período de até dois meses;

d) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado: impedimento pelo período de até quatro meses;

e) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta: impedimento pelo período de até seis meses;

f) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado; impedimento pelo período de até um ano.

9.2.4.1- A aplicação de três sanções de advertência pelo mesmo motivo, em um mesmo contrato, possibilita a aplicação da sanção de impedimento de licitar e contratar.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

9.2.5- Será aplicada a sanção de **declaração de inidoneidade** para licitar e contratar com a Administração Pública direta e indireta, de todos os entes federativos, pelo prazo mínimo de três anos e máximo de seis anos, observando-se os parâmetros estabelecidos, aos responsáveis pelas seguintes infrações:

a) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato: até quatro anos;

b) fraudar a licitação ou praticar ato fraudulento na execução do contrato; até seis anos;

c) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; até seis anos;

d) praticar atos ilícitos com vistas a frustrar os objetivos da licitação: até cinco anos;

e) praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, de 1º de agosto de 2013: até seis anos.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

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

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados pelos seguintes meios: preferencialmente na forma eletrônica, encaminhados para o e-mail licitacao@itabirito.cam.mg.gov.br ou no sítio eletrônico https://www.gov.br/compras/pt-br, ou protocolizados na Câmara Municipal de Itabirito, localizada na Avenida Queiroz Junior, nº 639, Bairro Praia, Itabirito/MG, de segunda à sexta-feira, de 12:00h às 18:00h, sob pena de não acolhimento.

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

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

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

11. DAS DISPOSIÇÕES GERAIS

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

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

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

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

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

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

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

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

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

11.10. **O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e no site https://www.itabirito.mg.leg.br/.**

11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

11.11.1. ANEXO I - Termo de Referência

11.11.2. ANEXO II – Estudo Técnico Preliminar

11.11.3. ANEXO III – Modelo de Proposta de Preços

11.11.4. ANEXO IV – Minuta de Termo de Contrato

Itabirito, 27 de dezembro de 2024.

CÂMARA MUNICIPAL DE ITABIRITO
ANDERSON MARTINS DA CONCEIÇÃO
Presidente da Câmara Municipal de Itabirito

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
(31) 3561-1599 - www.itabirito.mg.leg.br

CÂMARA MUNICIPAL DE ITABIRITO
Processo Administrativo n° 465/2024

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall e access point, para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara de Itabirito, em conformidade com as especificações técnicas e funcionais contidas nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

LOTE 1 – Firewall e Access Point						
ITE	**ESPECIFICAÇÃO**	**CATMAT**	**UNIDADE DE MEDIDA**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) – Firewall de Próxima Geração – Equipamento com suporte a cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo. Com 03 anos de suporte e garantia de hardware. Pacote de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para *appliance de Firewall de Próxima Geração (NGFW)* pelo prazo de	609340	Unidade	1	R$ 39680,88	R$ 39680,88

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

	36 (trinta e seis) meses.					
2	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) ou dispositivo remoto de ethernet – Firewall ou dispositivo deve oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. Deve funcionar em conjunto com o equipamento de firewall (item 01).	609340	Unidade	1	R$ 15461,00	R$ 15461,00
3	HARDWARE ACCESS POINT – Ponto de Acesso Wireless com Rádio Duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples, incluindo adaptador PoE.	605537	Unidade	8	R$ 7720,82	R$ 61766,53

LOTE 2 – Serviço de instalação, configuração e treinamento						
ITEMM	**ESPECIFICAÇÃO**	**CATSER**	**UNIDADE DE DE MEDIDA**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
4	Serviços de instalação, configuração, implantação e migração de regras de Firewall e Access Point.	26972	Unidade	1	R$ 18160,83	R$ 18160,83

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5	Treinamento de configuração, gerência e operação do Firewall. A transferência de conhecimento deve ter um total mínimo de 20 horas, feito por profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.	3840	Unidade	1	R$ 6200,00	R$ 6200,00
6	Serviços de suporte e assistência técnica para operação e gerenciamento do Firewall e Access Point.	26999	Mês	12	R$ 4518,17	R$ 4518,17

1.2. Os bens objeto desta contratação não é caracterizado como bem de luxo, conforme justificativa constante do Estudo Técnico Preliminar e critérios de sustentabilidade.

1.3. O prazo de vigência da contratação é de 12 (doze) meses contados da data de assinatura, prorrogável por até 05 (cinco) anos, na forma do artigo 106 da Lei n° 14.133, de 2021.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A fundamentação da contratação está sustentada na Lei nº 14.133/2021 – Lei de Licitações e Contratos Administrativos.

2.2. Esta contratação é justificada pela necessidade de atualização e adequação dos sistemas de segurança das redes de dados das unidades da Câmara Municipal de Itabirito e também pela demanda por acessibilidade de dispositivos por meio de conexão sem fio, com qualidade e com garantia de não interrupção dos serviços.

2.3. A sede da Câmara de Itabirito hoje possui o software pfSense como solução de Firewall. Apesar da vantagem deste sistema ser *open source*, ele não garante atualizações constantes nem a continuidade do serviço. Constantemente o Departamento de TI depara com o fato desta versão gratuita não atender as necessidades de controle e gerenciamento da rede. Há outros agravantes referentes a utilização deste software como, a necessidade de instalar e configurar diversos pacotes e plugins que não são nativos do sistema. Estas parametrizações são em sua maioria das vezes complexas de serem feitas. Por exemplo a instalação e manutenção dos módulos de monitoramento das atividades dos usuários, recursos para limitações de largura de banda, serviços de VPN, filtros de conteúdo e regras para detecção e prevenção de intrusão.

2.4. Além do mais, o servidor que hospeda o firewall pFSene é um computador genérico e convencional que possui um hardware insuficiente para atender o *throughput* exigido pela rede, ou seja, é um equipamento inadequado para ser utilizado para processar os pacotes que trafegam entre todos os dispositivos conectados e a internet.

2.5. O Centro de Atendimento ao Cidadão (CAC), o anexo da Câmara e os gabinete dos vereadores não possuem um sistema de firewall implantado em suas respectivas redes que são independentes. Portanto há uma carência nestes locais de um sistema que funcione como uma barreira de proteção contra invasões, ataques externos, guarda dos dados sensíveis, filtro de acessos e bloqueio de navegações suspeitas.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

2.6. A solução de firewall deve disponibilizar novos recursos customizados que permitam um melhor gerenciamento sobre as ameaças, facilidade na gestão e administração, interface intuitiva, suporte avançado personalizado e principalmente performance. Desta forma, faz-se necessária a adoção de um sistema moderno e robusto para manter os dados e informações da Câmara de Itabirito em segurança, protegendo contra invasões de hackers e evitando consequências que possam ser irreparáveis.

2.7. Para promover um gerenciamento centralizado de segurança apto a proteger a rede de ameaças externas e internas, bem como controlar o fluxo de dados entre essas redes e a Internet, a Câmara de Itabirito necessita de uma solução de firewall completa que permita:

2.7.1. Gerenciamento avançado dos níveis de serviços;

2.7.2. Visualização em tempo real das atividades exercidas na rede;

2.7.3. Diminuição de intervenções humanas;

2.7.4. Armazenamentos de históricos, gráficos e relatórios (por usuários e setores);

2.7.5. Priorização de tráfegos por protocolos e aplicações

2.7.6. Balanceamento entre links de internet e controle de banda

2.8. Outro objetivo importante é a adequação e preparação da estrutura do ambiente para comunicação junto a unidades externas, permitindo a unificação das redes da Câmara por meio de tecnologias como VPN, FTP, MPLS, VLAN. Esta opção irá facilitar o compartilhamento de arquivos entre os colaboradores e agilizar na comunicação por meio de ferramentas internas de produtividade, resultando na economia de recursos computacionais e centralizando todo o gerenciamento de acesso.

2.9. Portanto é fundamental a aquisição de solução integrada em segurança e proteção da rede computacional com características de APPLIANCE DE NEXT GENERATION FIREWALL – NGFW (Firewall de próxima Geração), com fornecimento de equipamentos, software para o gerenciamento centralizado e emissão de relatórios detalhados, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução, licenciamento do software para atualizações e repasse tecnológico através de treinamento.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

2.10. A modernização do ambiente computacional para acessibilidade dos equipamentos corporativos e não corporativos por meio da topologia sem fio também se tornou imprescindível. Atualmente são utilizados *access points* tradicionais que não são recomendados para ambientes institucionais por não possuírem níveis de segurança desejáveis, alto desempenho, confiabilidade, gerenciamento e recursos avançados de autenticação.

2.11. Os usuários dos gabinetes dos vereadores são desprovidos de conexão de acesso sem fio para dispositivos móveis e frequentemente estes colaboradores informam ao departamento de TI sobre a necessidade deste tipo de acesso. Ainda não foi disponibilizado este tipo de conexão devido a Câmara não possuir equipamento adequado para operar neste ambiente. Os *access points* tradicionais que temos não são compatíveis com o espaço em razão do alto número de usuários, área interna extensa e necessidade de um sistema de autenticação para atender a segurança da informação e aplicação da LGPD.

2.12. Outro agravante é o fato do sinal de telefone nesta região ser de baixa qualidade, diversas vezes não funciona, e cai constantemente deixando os colaboradores com uma comunicação precária por meio dos dispositivos móveis.

2.13. Portanto além do Firewall, há a necessidade de aquisição de equipamentos *access point* profissionais para promover a interconexão da rede cabeada com as diversas redes wireless da sede da Câmara, CAC, Anexo e gabinetes dos vereadores, uma vez que os dispositivos existentes na Câmara são inadequados.

2.14. Deste modo, esta contratação reflete uma necessidade evidente por recursos tecnológicos essenciais aos objetivos da Câmara de Itabirito, como medida eficaz, integrada, de ampliação e manutenção capaz de absorver as demandas, sempre crescentes, de capacidade, desempenho e disponibilidade, internas e externas, sem comprometer o resultado da prestação de serviços públicos.

2.15. O quantitativo ora definido foi baseado em um levantamento realizado pela equipe do Departamento de Tecnologia da Informação, tendo como base os equipamentos já existentes, já mencionados neste termo, bem como a necessidade de ampliação e modernização dos mesmos.

JUSTIFICATIVA PARA CONTRATAÇÃO POR MENOR PREÇO POR LOTE:

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

2.16. Justifica-se que o objeto seja contratado por menor preço por lote para assegurar a compatibilidade dos equipamentos e serviços e para que não haja prejuízo para o conjunto. Existem inúmeras marcas de equipamentos para compor um sistema Firewall e incontáveis modelos de Access Points no mercado e devido a essa diversidade há também vários tipos de configurações e métodos de instalação para que o sistema Firewall funcione em sincronia com os dispositivos de acesso sem fio.

2.17. O agrupamento dos itens evita que haja conflitos e incompatibilidade dos recursos tecnológicos pois cada fornecedor trabalha com equipamentos específicos e possuem diferentes metodologias de instalação. Não se demonstra viável para a administração licitar somente parte dos itens, pois todos os componentes deverão ser instalados em conjunto para que o sistema de segurança e de acesso funcionem de maneira correta. Além disso, os itens agrupados possuem similaridade e guardam relação entre si, não comprometendo a competitividade do certame.

2.18. Portanto a opção pela indivisibilidade do objeto é uma ação cautelosa definida pelo Departamento de Tecnologia da Informação desta casa legislativa que avaliou as peculiaridades envolvidas e identificou possíveis problemas na implantação do sistema. Todas análises foram feitas para assegurar a compatibilidade entre os itens e ainda assim manter a competitividade necessária à disputa, garantindo com que o licitante atue de forma independente.

2.19. O objeto da contratação está previsto no Plano de Contratações Anual 2023.

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

3.1. O presente Termo visa contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall e access point, para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara de Itabirito.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

3.2. A Câmara Municipal necessita dos serviços de atualização e adequação dos sistemas de segurança das redes de dados pois as versões gratuitas disponíveis não atendem as necessidades de controle e gerenciamento de rede e, ainda, não há atualmente equipamentos de hardware adequados para exercer as atividades de processamento de pacotes trafegados entre todos os dispositivos conectados e a internet. Há uma carência de um sistema que funcione como uma barreira de proteção contra invasões, ataques externos, guarda dos dados sensíveis, filtro de acessos e bloqueio de navegações suspeitas.

3.3. O serviço objeto do presente termo de referência, prevê a solução para os problemas ocasionados por eventuais invasões, ataques externos e atividades suspeitas.

3.4. A especificação do produto está descrita na planilha Lote 1 do item 1.1 e a especificação do serviço está descrita na planilha Lote 2 do item 1.1.

4. REQUISITOS DA CONTRATAÇÃO

Vistoria

4.1. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 12:00 às 18:00.

4.2. A solicitação de vistoria deverá ser encaminhada para o endereço camara@itabirito.cam.mg.gov.br indicando telefone para contato e agendamento.

4.3. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

4.4. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Sustentabilidade

4.5. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis.

Subcontratação

4.6. Não é admitida a subcontratação do objeto contratual.

Garantia da Contratação

4.7. Não haverá exigência da garantia da contratação dos arts. 96 e seguintes da Lei nº 14.133/21, em virtude da ausência de complexidade técnica e econômica que justifique sua adoção.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1 DESCRIÇÃO DE SOLUÇÃO DE SEGURANÇA DE REDE – NGFW (ITEM 1)

4.1.1 Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares*, Filtro de URL, criptografia de e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.

4.1.2 Dispositivo remoto de ethernet, para oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos.

4.1.3 Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / *malwares,* assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

aplicação web sem custo adicional, pelo período mínimo de 36 (trinta e seis) meses.

4.1.4 Para os itens que representem bens materiais, a **CONTRATADA** deverá fornecer produtos novos, sem uso anterior.

4.1.5 Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

4.1.6 Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

4.1.7 Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento.

4.1.8 Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).

4.1.9 Por alta disponibilidade (HA) entende-se que a solução deverá ser composta ao menos por dois *appliances*, licenciados para funcionamento em redundância.

4.1.10 A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um equipamento (sempre em modo de alta disponibilidade HA) para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.

4.1.11 Cada *appliance* deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

4.1.12 O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

5.2- DESCRIÇÃO E CARACTERÍSTICAS DE FIREWALL (NGFW) OU DISPOSITIVO REMOTO DE ETHERNET (ITEM 2)

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.2-1. Deve ser do mesmo fabricante do firewall e em forma de appliance.

5.2-2. Deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso aos recursos remotos.

5.2-2.1. O túnel seguro deve ter no mínimo 850 Mbps de throughput utilizando criptografia AES256 e TLS 1.2.

5.2-2.2. Deve suportar módulo adicional de Wi-fi MIMO 2x2:2, com rádio padrão mínimo 802.11 a/b/g/n/ac Wave 1 (Wi-Fi 5), habilitado para banda dupla ou 4G/LTE.

5.2-2.3. Deve possuir no mínimo 04(quatro) interfaces 10/100/1000 Base-TX (1 GbE de cobre).

5.2-2.4. Deve possuir no mínimo 02(duas) interfaces USB 3.0. Possuir luzes indicativas no mínimo equipamento ligado, interface de rede ligada.

5.2-2.5. Possuir fonte de alimentação bivolt compatível com 110-240 V, 50-60 Hz. (RED15/REDE15w).

5.2-2.6. Deve suportar 2a fonte de alimentação.

5.2-2.7. Possuir no mínimo as certificações CE/FCC/IC/RCM/VCCI/CB/UL/CCC/KC/ANATEL.

5.2-2.8. Operar com humidade de no mínimo entre 10% a 90%, sem condensação.

5.2-2.9. Deve ser possível ser gerenciado pelo equipamento concentrador.

5.2-2.10. Deve ser possível pelo equipamento concentrador atualizar todos os firmwares de forma a facilitar a manutenção.

5.2-2.11. Deve ser permitir carregar a configuração por USB ou de forma automática.

5.2-2.12. Uplink deve permitir a configuração estática de IP ou através de DHCP.

5.2-2.13. Deve possuir a funcionalidade de gerenciar o DHCP de forma centralizada.

5.2-2.14. Deve possuir alta disponibilidade implementando fail-over nos túneis com a matriz.

5.2-2.15. Deve possuir a funcionalidade de balanceamento entre dois túneis com a matriz.

5.2-2.16. Para facilitar a implementação de regras específicas por regiões deve aparecer como interface no concentrador central.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.2-2.17. Para facilitar a implementação de regras específicas deve possuir funcionalidade de agregar logicamente todas as localidades como uma interface no concentrador central.

5.2-2.18. Deve ter a funcionalidade de compressão do túnel de forma a otimizar a banda utilizada.

5.2-2.19. Deve possuir a funcionalidade de filtrar por MAC.

5.3- CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DO FIREWALL DE PRÓXIMA GERAÇÃO - NGFW

5.3-1. Performance mínima de 10.500 Mbps de *throughput* para firewall.

5.3-2. Performance mínima de 2.500 Mbps de throughput para firewall NGFW.

5.3-3. Performance mínima de 3.250 Mbps de throughput de IPS.

5.3-4. Performance mínima de 900 Mbps de throughput para controle de AV/proxy.

5.3-5. Performance mínima de 1.800 Mbps de throughput de VPN.

5.3-6. Suporte a, no mínimo, 5.000.000 (5 milhões) de conexões simultâneas.

5.3-7. Suporte a, no mínimo, 69.900 (sessenta e nove mil e novecentos) novas conexões por segundo.

5.3-8. Possuir o número irrestrito quanto ao máximo de usuários licenciados.

5.3-9. Possuir armazenamento interno de no mínimo 64 GB SSD para sistema operacional, quarentena local, logs e relatórios.

5.3-10. Possuir no mínimo 4GB de memória RAM.

5.3-11. Possuir no mínimo 12 (doze) interfaces de rede GbE1000Base-TX.

5.3-12. Possuir no mínimo 2 (duas) interfaces SFP Fiber.

5.3-13. Possuir no mínimo 1 (um) módulo de expansão de interfaces.

5.3-14. Possuir 1 (uma) interface do tipo console ou similar.

5.4- CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO

5.4-1. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.4-2. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), console de gerência, monitoração e logs.

5.4-3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários, controle granular de permissões, IPS, Firewall, Antispam, VPN IPSec, SSL VPN e SSL Inspection.

5.4-4. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação técnica.

5.4-5. Todos os equipamentos fornecidos poderão ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

5.4-6. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

5.4-7. O software deverá ser fornecido em sua versão mais atualizada.

5.4-8. A solução deverá ter capacidade de operar em alta Disponibilidade (HA). O HA deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.

5.4-9. Uma interface completa de comando de linha (*CLI command-line-interface*) deverá ser acessível através da interface gráfica e via porta serial.

5.4-10. A atualização de software deverá enviar avisos de atualização automáticos.

5.4-11. O sistema de objetos deverá permitir a definição de redes, serviços, *hosts* períodos de tempos, usuários e grupos, clientes e servidores.

5.4-12. O *backup* e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

5.4-13. As notificações deverão ser realizadas via e-mail e SNMP.

5.4-14. Suportar SNMPv3 e Netflow.

5.4-15. O firewall deverá ser *stateful*, com inspeção profunda de pacotes.

5.4-16. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

5.4-17. As políticas de NAT deverão ser customizáveis para cada regra.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.4-18. A proteção contra *flood* deverá ter proteção contra DoS (*Denial of Service*), DdoS (*Distributed DoS*).

5.4-19. Proteção contra *anti-spoofing*.

5.4-20. Suportar IPv4 e IPv6.

5.4-21. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e *IPv6 Rapid Deployment (6rd)* de acordo com a RFC 5969.

5.4-22. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).

5.4-23. Deve possuir tecnologia de conectividade SD-WAN;

5.4-24. A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN;

5.4-25. Deve implementar balanceamento entre os links WAN com método SpillOver;

5.4-26. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN;

5.4-27. Deve suportar o uso de, no mínimo, 3 (três) links;

5.4-28. Deve suportar o uso de links de interfaces físicas, subinterfaces lógicas de VLAN e túneis IPSec;

5.4-29. Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde;

5.4-30. A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

5.4-31. A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima;

5.4-32. Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês;

5.4-33. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado;

5.4-34. A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.4-35. Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;

5.4-36. A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados;

5.4-37. Deve possibilitar o roteamento baseado em VPNs;

5.4-38. Deve suportar criar políticas de roteamento;

5.4-39. Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:

5.4-39.1. Interface de entrada do pacote;

5.4-39.2. IPs de origem;

5.4-39.3. IPs de destino;

5.4-39.4. Portas de destino;

5.4-39.5. Usuários ou grupos de usuários;

5.4-39.6. Aplicação em camada 7.

5.4-40. Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento;

5.4-41. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e *tagging* de VLAN.

5.4-42. Deve suportar Extended VLAN;

5.4-43. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, *failover* automático e balanceamento por peso.

5.4-44. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

5.4-45. Deve permitir a configuração de jumbo frames nas interfaces de rede;

5.4-46. Deve permitir a criação de um grupo de portas layer2;

5.4-47. A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.4-48. A solução deverá permitir configurar os serviços de DNS, *Dynamic* DNS, DHCP e NTP;

5.4-49. O *traffic shapping (QoS)* deverá ser baseado em rede ou usuário.

5.4-50. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

5.4-51. Deve possuir otimização em tempo real de voz sobre IP.

5.4-52. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

5.5- CONTROLE POR POLÍTICAS DE FIREWALL

5.5-1. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

5.5-2. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

5.5-3. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

5.5-4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

5.5-5. Controle de políticas por países via localização por IP.

5.5-6. Suporte a objetos e regras IPV6.

5.5-7. Suporte a objetos e regras *multicast*.

5.6- PREVENÇÃO DE AMEAÇAS

5.6-1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, *Anti-Malware* e Firewall de Proteção Web (*WAF*) integrados no próprio *appliance* de Firewall ou entregue em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

5.6-2. Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

5.6-3. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.6-4. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

5.6-5. Deve suportar granularidade nas políticas de IPS Antivírus e *Anti-Malware*, possibilitando a criação de diferentes politicas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;

5.6-6. A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em núvem;

5.6-7. Para a eficácia da análise de malwares Zero-Days, a solução de Sandobox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning;

5.6-8. A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma;

5.6-9. Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em núvem;

5.6-10. A proteção *Anti-Malware* deverá bloquear todas as formas de vírus, *web malwares*, *trojans* e *spyware* em HTTP e HTTPS, FTP e *web-e-mails*.

5.6-11. A proteção Anti-Malware deverá realizar a proteção com emulação *JavaScript*.

5.6-12. Deve ter proteção em tempo real contra novas ameaças criadas.

5.6-13. Deve possuir pelo menos duas *engines* de anti-vírus independentes e de diferentes fabricantes para a detecção de *malware*, podendo ser configuradas isoladamente ou simultaneamente.

5.6-14. Deve permitir o bloqueio de vulnerabilidades.

5.6-15. Deve permitir o bloqueio de *exploits* conhecidos.

5.6-16. Deve detectar e bloquear o tráfego de rede que busque acesso a *command and control* e servidores de controle utilizando múltiplas camadas de DNS, *AFC* e firewall.

5.6-17. Deve incluir proteção contra-ataques de negação de serviços.

5.6-18. Ser imune e capaz de impedir ataques básicos como: *SYN flood, ICMP flood, UDP Flood*, etc.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.6-19. Suportar bloqueio de arquivos por tipo.

5.6-20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

5.6-21. Os eventos devem identificar o país de onde partiu a ameaça.

5.6-22. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.

5.6-23. O equipamento do tipo 1 deve ter a capacidade de atuar como um gateway AntiSpam de modo que possa realizar filtragens dos e-mails e aplicar políticas.

5.6-24. O gateway de e-mail incluso no equipamento do tipo 1 deve ter pelo menos as seguintes proteções:

5.6-25. Sender Policy Framework (SPF);

5.6-26. Domain Keys Identified Mail (DKIM);

5.6-27. Domain-based Message Authentication, Reporting & Conformance (DMARC);

5.6-28. Bounce Address Tag Validation (BATV);

5.6-29. O filtro de e-mail deve quarentenar os e-mails suspeitos ou realmente maliciosos;

5.6-30. A solução deve possibilitar aos usuários acessarem um painel para verificação da sua caixa pessoal de quarentena, possibilitando então a liberação ou a exclusão das mensagens;

5.6-31. A função de AntiSpam deve permitir a configuração de relays com a possibilidade de autenticação deles;

5.6-32. A função de AntiSpam deve possibilitar também o envio de e-mails seguros, realizando a criptografia das mensagens bem como dos seus anexos.

5.6-33. A função de AntiSpam deve conter funcionalidades de prevenção a perda de dados (DLP) para evitar que informações sigilosas sejam vazadas;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.6-34. O equipamento deverá possuir firewall de aplicação Web (*WAF*) com a função de *reverse proxy*, função de *URL hardening* realizando *deep-linking* e prevenção dos ataques de *path traversal* ou *directory traversal*.

5.6-35. O firewall de aplicação Web (*WAF*) deverá realizar *cookie signing* com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.

5.6-36. O firewall de aplicação Web (*WAF*) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do *WAF* e permissão e bloqueio de *ranges* de IP.

5.6-37. Deverá permitir a identificação dos IPs de origem através de proxy via "X-forward headers".

5.6-38. Deve possuir pelo menos duas *engines* de antivírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.

5.6-39. Proteção pelo menos contra os seguintes ataques, mas não limitado a: *SQL injection* e *Cross-site scripting*.

5.7- CONTROLE E PROTEÇÃO DE APLICAÇÕES

5.7-1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, *port hopping* e túnel através de tráfego SSL encriptado.

5.7-2. Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3.

5.7-3. O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

5.7-4. O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.7-5. Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

5.7-6. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

5.7-7. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website).

5.7-8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

5.7-9. Atualizar a base de assinaturas de aplicações automaticamente.

5.7-10. Reconhecer aplicações em IPv6.

5.7-11. Limitar a banda usada por aplicações (*traffic shaping*).

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.7-12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários.

5.7-13. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

5.7-14. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuem acesso a estes aplicativos devem ter a utilização bloqueada.

5.8- CONTROLE E PROTEÇÃO WEB

5.8-1. Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

5.8-2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

5.8-3. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, Radius, *E-directory* e base de dados local;

5.8-4. Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius;

5.8-5. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

5.8-6. Possuir pelo menos 90 categorias de URLs;

5.8-7. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

5.8-8. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.8-9. Deve ser capaz de forçar as restrições do Youtube

5.8-10. Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;

5.8-11. Suportar a criação categorias de URLs customizadas;

5.8-12. Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

5.8-13. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada

5.8-14. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

5.8-15. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

5.8-16. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;

5.8-17. Deve realizar caching do conteúdo web;

5.8-18. Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

5.8-19. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet.

5.8-20. A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

5.8-21. Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual.

5.8-22. A solução deve permitir o enforce dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar.

5.9- IDENTIFICAÇÃO DE USUÁRIOS

5.9-1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

serviços de diretório, autenticando via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

5.9-2. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).

5.9-3. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

5.9-4. Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

5.9-5. Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, afim de garantir que usuários logados em servidores de multi sessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas um IP de origem;

5.9-6. Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.

5.9-7. Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

5.10- **QUALIDADE DE SERVIÇO – QoS**

5.10-1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.10-2. *A solução deverá suportar Traffic Shaping* (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

5.10-3. Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e *bit rate* de modo individual ou compartilhado.

5.10-4. Suportar priorização *Real-Time* de protocolos de voz (VoIP).

5.10-5. Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

5.11- **REDES VIRTUAIS PRIVADAS – VPN**

5.11-1. Suportar VPN *Site-to-Site e Cliente-to-Site*.

5.11-2. Suportar IPsec VPN.

5.11-3. Suportar SSL VPN.

5.11-4. Suportar L2TP e PPTP.

5.11-5. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

5.11-6. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

5.11-7. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.

5.11-8. Deve possuir opção de VPN IPSEC com aplicação nativa do fabricante.

5.11-9. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

5.11-10. A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;*Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (*Advanced Encryption Standard*); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.11-11. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.

5.11-12. Deve suportar nativamente a integração com a Amazon, a fim de estabelecer um túnel seguro entre os equipamentos e a VPN da AWS.

5.11-13. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-Malware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

5.11-14. Suportar autenticação via AD/LDAP, *Token* e base de usuários local;

5.11-15. Permitir estabelecer um túnel SSL VPN com uma solução de autienticação via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local.

5.12- **GERÊNCIA ADMINISTRATIVA CENTRALIZADA**

5.12-1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

5.12-2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

5.12-3. Estar licenciada para gerenciar as soluções de firewall de próxima geração.

5.12-4. Devem ser fornecidas soluções virtuais, em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação.

5.12-5. Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração, sem necessidade de acesso direto aos equipamentos.

5.12-6. Deve permitir a criação de Templates para configurações.

5.12-7. Deve possuir indicadores do estado de equipamentos e rede.

5.12-8. Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

5.12-9. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.12-10. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

5.12-11. Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas;

5.12-12. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

5.12-13. Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

5.12-14. Deve possibilitar o envio dos logs via syslog com conexão segura (TLS).

5.13- GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS

5.13-1. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

5.13-2. Estar licenciada para gerenciar as soluções de firewall de próxima geração.

5.13-3. Devem ser fornecidas soluções virtuais, em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 2TB de dados.

5.13-4. Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

5.13-5. Deve possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

5.13-6. Deve conter relatórios pré configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;

5.13-7. Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.13-8. Deve conter customizações dos relatórios para inserção de logotipos próprios.

5.13-9. Deve fornecer relatórios de compliance SOX, HIPAA e PCI.

5.13-10. Deve permitir a exportação via PDF ou Excel.

5.13-11. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

5.13-12. Deve fornecer relatórios de tendências.

5.13-13. Deve fornecer logs em tempo real, de auditoria e arquivados.

5.13-14. Deve possuir mecanismo de procura de logs arquivados.

5.13-15. Deve ter acesso baseado em Web com controles administrativos distintos.

5.14- INTEGRAÇÃO COM SOLUÇÃO DE ENDPOINT

5.14-1. A solução de firewall deve possibilitar a integração com a atual solução de Endpoint (Sophos Cloud) instalada no ambiente da contratante.

5.14-2. A integração deve possibilitar a criação de regras de bloqueio de endpoints, com determinado status, dentro do Firewall de forma automática, sem que haja intervenção por parte do time da contratante.

5.14-3. A integração deverá ser nativa entre o firewall e o endpoint, ou utilizando APIs de integração da solução de firewall.

5.14-4. Caso a integração não seja nativa, cabe a CONTRATADA:

5.14-4.1. Desenvolver completamente a solução de integração do Firewall e o Endpoint instalado (Sophos Cloud);

5.14-4.2. O Software de integração deve realizar a criação das regras do Firewall com no máximo 2 (dois) minutos após o incidente detectado no Endpoint;

5.14-5. Possuir interface WEB, acessada por HTTP ou HTTPS, para definição dos objetos das regras a serem criados, com no mínimo origem, destino, status do endpoint e protocolos;

5.14-6. Possibilitar o envio de e-mails sobre as ações do software;

5.14-7. Entregar o software de integração em máquina virtual, Windows ou Linux, juntamente com as devidas licenças necessárias para sistemas operacionais, banco de dados, etc;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.14-8. A máquina virtual será instada no ambiente da contratante, não sendo permitido soluções em nuvem;

5.14-9. A máquina virtual não deverá ter qualquer acesso remoto que não seja acordado pela contratante;

5.14-10. A mesma não deverá enviar/receber pacotes TCP/UDP ou por qualquer outro meio de comunicação, que não sejam os objetos de Firewall deste edital ou a console do endpoint da contratante;

5.14-11. A gestão do sistema operacional da máquina virtual em questão será de inteira responsabilidade da contratante, de modo a garantir que sejam realizados todos os updates, correções de patchs, segurança do sistema operacional, bem como com seus softwares, alterações de versões, etc;

5.14-12. A máquina virtual deve ser utilizada única e exclusivamente para o fim proposto no edital, não sendo permitido que a máquina virtual realize qualquer outra função;

5.14-13. Permitir backup das configurações do software de integração, possibilitando o restore em outra máquina virtual de forma a não comprometer o ambiente;

5.14-14. Realizar manutenção/alteração total no software de integração, sem custo adicional, durante o período de vigência do suporte do Firewall Tipo 1;

5.14-15. Realizar teste de bancada, a fim de comprovar a efetividade da integração;

5.14-16. Possuir atendimento 24 horas por dia, 07 dias por semana (24x7), durante todos os dias do ano, inclusive feriados;

5.14-17. O atendimento deve ser realizado por telefone, e-mail, remoto ou on-site (ilimitado);

5.14-18. Apresentar SLA em contrato com os seguintes tempos:

5.14-18.1. Criticidade Baixa – Tempo de resposta de até 6 horas e até 48 horas para tempo de solução. Os casos definidos com criticidade baixa são: Falha na console de acesso Web do software de integração, alterações no funcionamento da ferramenta mediante solicitação da contratada, falhas no envio de e-mails por parte do software de integração.

5.14-18.2. Criticidade Média - Tempo de resposta de 4 horas e até 8 horas para tempo de solução. Os casos definidos com criticidade média são: Bloqueios

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

inesperados realizados pelo software de integração, falha na identificação do status dos endpoints, falha no job de backup.

5.14-18.3. Criticidade Alta – Tempo de resposta de até 2 horas e até 6 horas para tempo de solução. Os casos definidos com criticidade alta são: Sistema operacional da máquina virtual do software de integração inoperante, com problemas durante o boot da VM, qualquer falha no software que comprometa o funcionamento da solução como um todo.

5.15- **CARACTERÍSTICAS ESPECÍFICAS DO HARDWARE ACCESS POINT (ITEM 3)**

5.15-1. Equipamento deve proporcionar o máximo em segurança e desempenho de rede.

5.15-2. Padrão / Normas WLAN: 802.11ax, Wi-Fi 6

5.15-3. Gerenciamento por meio de plataforma central da fabricante e por interface web local.

5.15-4. Indicado para instalação em ambiente fechado.

5.15-5. Deve permitir ser implantado montado em mesa, parede ou teto.

5.15-6. Rádio duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples

5.15-7. Deve possuir ao menos 4 antenas omnidirecionais internas, sendo: 2x antenas 2,4 GHz e 2x antenas 5 GHz.

5.15-8. Deve possuir tecnologia DFS (Dynamic Frequency Selection) para gerenciar o uso de frequências de rádio.

5.15-9. Desempenho: 2x 2:2.

5.15-10. Taxas máximas de transmissão: 2975 Mbps sendo 575 Mbps (2,4 GHz) +2400 Mbps (5 GHz).

5.15-11. Interfaces: 1x 12V DC-in, 1x porta Gigabit Ethernet com 802.3at PoE+, Console Micro-USB.

5.15-12. Deve ser ter plataforma na nuvem escalonável que permita o gerenciamento remoto.

5.15-13. Deve possuir recurso de resposta a ameaças ativas para isolamento de hosts comprometidos.

5.15-14. Deve possuir portal cativo para acesso de convidados e visitantes.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.15-15. Deve permitir o gerenciamento centralizado juntamente com o ecossistema completo das soluções de segurança cibernética da fabricante.

5.15-16. Deve permitir Múltiplos SSIDs.

5.15-17. Deve permitir SSIDs com base em tempo (hora do dia, dia da semana).

5.15-18. Deve permitir Balanceamento de carga do cliente.

5.15-19. Deve permitir Seleção automática de canais.

5.15-20. Deve permitir Seleção de largura do canal.

5.15-21. Deve permitir Direção de banda

5.15-22. Deve permitir Airtime Fairness.

5.15-23. Deve permitir Assistente de roaming (802.11r).

5.15-24. Deve permitir Transição rápida (802.11r).

5.15-25. Deve permitir Portal Cativo: Personalização da página inicial (logotipo, nome, mensagem de boas-vindas, termos e condições).

5.15-26. Deve ser Uniusuário MIMO (SU-MIMO) e Multiusuário MIMO (MU-MIMO).

5.15-27. Deve permitir ter os recursos 802.11 avançados como: Coloração BSS (Basic Service Set), Uplink/Downlink OFDMA e TWT (Target Wake Time).

5.15-28. Deve ter os seguintes recursos de Log e Monitoramento: Captura de Pacotes, Logs de auditoria de Syslog, Log e relatórios de eventos (Relatórios de Syslog), Identidade do usuário (Autenticação baseada no usuário), Detecção de AP ilegítimo.

5.15-29. Deve ter os seguintes recursos de autenticação do usuário / dispositivo: WPA3-Personal SAE, WPA3 Enterprise and Enhanced Open (OWE), Autenticação Enterprise (RADIUS), Filtragem de MAC, Senha diária, semanal, mensal, Autenticação de Backend, Voucher com base em tempo e em cota (de dados), Login via rede social, Isolamento de Cliente, Portal Cativo: Jardim Murado, Rede de convidado – modo de ponte.

5.15-30. Deve ter os seguintes recursos de rede: ARP proxy, Suporte a VLAN, Conversão multicast para unicast, Interface LAG (Link Aggregation Group).

5.15-31. Requisito de energia (PSE) / Potência (máx): 17,5W

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.15-32. Deve ter certificações e conformidades: CB, UL, CE, FCC, ISED, RCM, TEC, EN 60601-1-2 (Diretiva de Equipamentos Médicos).

5.15-33. Deve permitir alimentação elétrica por meio de Power Over Ethernet, padrão 802.3at (Poe +).

5.15-34. O adaptador PoE deve estar incluso como assessório do equipamento.

5.15-35. Padrão PoE mínimo deve ser 30W por porta.

5.15-36. Deve ser fornecido com kit de montagem incluindo: suporte para montagem em parede e teto (barra T de 15/16'' ou 9/16'') e kits para teto plano, plenum e montagem suspensa.

5.15-37. Licenciamento console de controle: Compatível e integrado com o Firewall.

5.15-38.

5.16- **GARANTIA E ASSISTÊNCIA TÉCNICA**

5.16-1. A Garantia dos equipamentos fornecidos deverá ser realizada pelo fabricante pelo prazo de 03 (três) anos, com assistência técnica e solução no prazo máximo de 06 (seis) horas, para o lote 01, comprovados através de declaração do fabricante a garantia ofertada.

5.16-2. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

5.16-3. A assistência técnica dos equipamentos deverá ser executada pelo fabricante ou empresa credenciada pelo mesmo, comprovado através de declaração do fabricante assumindo a assistência técnica durante a garantia e, no caso, de execução por parte de empresa credenciada, indicar a empresa com os correspondentes contatos.

SERVIÇOS

5.17- **SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E IMPLANTAÇÃO DO FIREWALL E ACCESS POINT**

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.17-1. Todos os equipamentos do Lote 1 deverão ser instalados, configurados e ativados pela CONTRATADA nos locais indicados pela Câmara de Itabirito. Os serviços de instalação e configuração da solução poderão ser executados nos seguintes endereços: Sede da Câmara de Itabirito localizada na Av. Queiroz Junior nº 639, Bairro Praia, Itabirito MG. Centro de atendimento ao Cidadão e Gabinete dos Vereadores localizados na rua José Benedito n°189 - 3° andar, bairro Santa Efigênia, Itabirito MG.

5.17-2. A instalação deverá ser previamente agendada com o gestor do contrato e deverá acontecer em dias úteis no horário de 12:00 às 18:00.

5.17-3. A CONTRATADA deverá realizar os serviços de instalação e configuração dos equipamentos e licenciamentos de forma a garantir o seu pleno funcionamento no ambiente tecnológico da Câmara de Itabirito.

5.17-4. O planejamento, instalação, configuração e ativação dos equipamentos deverão ser executados por profissionais qualificados e a empresa deverá ser credenciada pelo fabricante dos equipamentos.

5.17-5. A CONTRATADA deverá garantir todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue.

5.17-6. Todas as configurações serão realizadas em conformidade com a recomendação do fabricante dos equipamentos e softwares da solução existente, boas práticas de implementação recomendada pelo fabricante e os requisitos fornecidos pela Câmara de Itabirito ao ambiente em questão.

5.17-7. Todos os equipamentos adquiridos na solução deverão ser instalados, configurados, testados e integrados na estrutura existente (rede de dados) da Câmara de Itabirito, garantindo assim a total compatibilidade e interoperabilidade de sua infraestrutura.

5.17-8. A contratada deverá realizar as transferências de regras e migrações de parâmetros existentes nos firewalls atuais mediante disponibilização de acesso e acompanhamento técnico da contratante. Os equipamentos firewalls utilizados atualmente no ambiente da contratante são: 1 servidor físico pfSense e 1 Routerboard Mikrotik RB750Gr3, ambos utilizados em topologia bastion host (o firewall está localizado entre a internet e o segmento de rede interna).

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.17-9. Os equipamentos e serviços serão aceitos mediante comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos e a solução se encontre em operação plena. Essa comprovação será realizada por meio de observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações.

5.17-10. A CONTRATADA deverá fornecer catálogos, manuais e/ou prospectos (em formato físico ou digital) de todos os materiais e equipamentos entregues.

5.17-11. Na execução do serviço, deve estar inclusa pela CONTRATADA toda mão de obra necessária para instalação física e configuração dos equipamentos para o funcionamento pleno dos Access Point.

5.17-12. Deve ser realizado pela CONTRATADA toda a estrutura de cabeamento de redes de dados para interligação entre a área de instalação do Access Point e o backbone da Câmara de Itabirito.

5.17-13. A CONTRATADA, se necessário, deverá prover a instalação de pontos de elétrica para a interligação do access point até o quadro de distribuição de energia existente na estrutura da Câmara de Itabirito.

5.17-14. Deve ser fornecido pela CONTRATADA, caso necessário, material para a instalação dos Access Point como buchas, parafusos, conectores, eletrodutos, conduletes, canaletas, tomadas, cabos, caixas sistema x, tampas, espelhos e suportes.

5.17-15. Deve ser providenciado pela contratada qualquer eventual serviço necessário para execução da instalação física dos Access Point como, por exemplo, furos e reparos em alvenarias ou gessos.

5.17-16. Deve incluir a fixação de equipamentos e materiais com o devido acabamento necessário em conformidade com a arquitetura presente no ambiente.

5.17-17. A contratante irá disponibilizar espaço no rack / armário para abrigar o equipamento Hardware Firewall. Caso não haja espaço será fornecido um novo rack / armário pela contratante para ser instalado pela contratada.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.17-18. Caberá, portanto, a CONTRATADA a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos do lote 1.

5.17-19. A CONTRATADA deverá designar um profissional Técnico Responsável para acompanhar a execução dos serviços desde o planeamento até a implantação da solução.

5.17-20. Após as fases de implantação dos equipamentos, a equipe técnica da CONTRATADA deverá realizar a transferência tecnológica da solução à equipe técnica da Câmara de Itabirito.

5.17-21. A CONTRATADA deve realizar o teste de funcionamento dos equipamentos, após sua instalação, na presença do contratante.

5.17-22. Todos os serviços de instalação, configuração e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

5.17-23. Durante os primeiros 2 (dois) dias úteis após a instalação e ativação do sistema, a CONTRATADA deverá manter, no mínimo, 01 (um) técnico para a operação assistida e fornecimento de suporte, nas dependências da Câmara de Itabirito, sem custo adicional para a Autarquia.

5.17-24. Caberá à CONTRATADA a realização dos demais serviços necessários ao pleno funcionamento da solução fornecida.

5.17-25. Adicionalmente a CONTRATADA deverá:

5.17-25.1. Planejar a instalação e implantação da solução e elaborar o cronograma;

5.17-25.2. Instalar os equipamentos de acordo com a proposta de hardware deste termo;

5.17-25.3. Implantar o firewall de nova geração, migrar as configurações existentes para o mesmo e vincular ao AD;

5.17-25.4. Integrar o firewall aos endpoints;

5.17-25.5. Instalação física e lógica;

5.17-25.6. Instalar Cabling e alimentação elétrica dos ativos;

5.17-25.7. Configuração de regras, a serem definidas com o time;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.17-25.8. Validações de regras;

5.17-25.9. Entregar da documentação pertinente: relatório conclusivo com as configurações e parâmetros definidos bem como um resumo de toda a implementação.

5.17-26. Os serviços deverão ser realizados no prazo máximo de 15 (quinze) dias úteis após a data da entrega dos equipamentos.

5.17-27. Realizar o acompanhamento, suporte, e assistência técnica pós instalação por 12 meses, contemplando ajustes de configurações, dúvidas, recuperação de desastres, novas instalações.

5.17-28. Todos os serviços de instalação e configuração deverão ser executados de forma presencial, por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

5.18- SERVIÇO DE TREINAMENTO

5.18-1. Deverá ser realizado programa de treinamento, de forma a capacitar os profissionais da Câmara de Itabirito na utilização dos equipamentos e softwares envolvidos na solução ofertada.

5.18-2. A contratada deve realizar treinamento com transferência de conhecimento para no mínimo 2 pessoas com no mínimo de 32 horas (incluídos nessas horas as 16 horas de implantação assistida).

5.18-3. O treinamento deverá abranger todos os equipamentos, componentes e softwares da solução ofertada, em seus aspectos mais relevantes como instalação, configuração e gerenciamento, tomando por base a Documentação do Projeto, e ainda contemplando princípios básicos de funcionamento, noções de manuseio, operação e conservação, principais comandos e procedimentos diários de operação, procedimentos de emergência a serem executados em casos de contingência, geração, emissão e análise de relatórios.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.18-4. A CONTRATADA fornecerá treinamento aos colaboradores da CONTRATANTE, com instrutor certificado pelo fabricante, buscando garantir a utilização de práticas corretas na operação do ambiente e a correta reação nos casos de incidentes envolvendo os sistemas do Data Center.

5.18-5. O escopo do plano de treinamento para instalação, operação e configuração, gerenciamento centralizado e gerenciamento de relatórios deve prever:

5.18-5.1. Informativo global dos componentes tecnológicos envolvidos na prestação dos serviços contratados;

5.18-5.2. Compreensão geral da filosofia de funcionamento e de operação;

5.18-5.3. Conhecimento e usabilidade dos recursos (hardwares e softwares) envolvidos;

5.18-5.4. Funcionalidades do Sistema em seus respectivos módulos.

5.18-5.5. Reinstalação, implantação e configuração dos equipamentos de Firewall e Access Point;

5.18-5.6. Parametrização, criação de regras, backups, gerenciamento dos equipamentos de Firewall e Access Point;

5.18-5.7. Gerenciamento, monitoramento e emissão de relatórios e logs da solução do objeto da contratação.

5.18-6. O treinamento deverá ser ministrado em local, data e horário indicado pela CONTRATANTE, de modo que o aluno possa praticar, ao menos, a configuração, o gerenciamento e a operação dos equipamentos, soluções e softwares que compõem o data center;

5.18-7. A capacitação na solução deverá acontecer no prazo máximo de 30 (trinta) dias após a instalação e configuração dos equipamentos, no local de instalação dos equipamentos.

5.18-8. Todos os serviços de treinamento e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

5.19- SERVIÇO DE SUPORTE TÉCNICO

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

5.19-1. Serviços de suporte técnico deve ser prestado pela contratada. Este serviço se difere da assistência técnica de hardware do fabricante e garantia que estão incluídos na subscrição dos equipamentos.

5.19-2. Durante o período de suporte técnico, a CONTRATANTE poderá solicitar o suporte técnico remoto ou presencial especializado a contratada, com limite de 4 (quatro) visitas presenciais por mês;

5.19-3. A solicitação de suporte técnico por parte da contratada se dará através de abertura de chamado, a ser realizado por, no mínimo, os seguintes meios de comunicação, disponibilizados sempre em idioma português (Brasil):

5.19-3.1. Ligação telefônica;

5.19-3.2. Sistema web (website) com autenticação segura (mínimo usuário e senha de acesso);

5.19-3.3. E-mail corporativo (em caso de indisponibilidade dos meios anteriormente citados);

5.19-4. O suporte técnico deverá estar disponível na modalidade “5x7” (2ª à 6ª, horário comercial);

5.19-5. A CONTRATADA deverá realizar mensalmente manutenções preventivas, inspeções e conferência dos parâmetros dos equipamentos de forma a garantir o pleno funcionamento e assegurar que as configurações de segurança estejam sendo aplicadas conforme critérios definidos durante a implantação.

5.19-6. O suporte deverá respeitar, no mínimo, os seguintes tempos de resposta para os níveis de severidade abaixo:

5.19-6.1. Crítica: solução inoperante ou falha de grande impacto causando parada na solução - Atendimento em até 2(duas) horas, com solução em até 6 (seis) horas;

5.19-6.2. Alta: incidentes que causem danos moderados à solução, como lentidão elevada, travamentos, interrupções recorrentes - Atendimento em até 4(quatro) horas, com solução em até 8 (oito) horas;

5.19-6.3. Baixa ou informativa: incidentes de baixo impacto, como lentidão esporádica, erros em ferramenta de geração de relatórios. Inclui também chamados para esclarecimento de dúvidas sobre a configuração e/ou

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

funcionamento da solução - Para este nível de severidade o tempo de resposta deverá ser de até 2 (dois) dias, em horário comercial.

5.19-6.4. O serviço de suporte técnico deverá ser realizado pelo período 12 meses, que será contado após a validação pela contratante da entrega dos serviços de instalação (item 4) e serviço de treinamento (item 5) pela contratada.

5.19-6.5. O serviço de suporte técnico será pago de forma mensal pela contratante sendo dividido por 12 parcelas do valor total proposta pela contratada.

5.19-6.6. Os serviços de suporte técnico deverão ser executados por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

SIGILO E PROPRIEDADE DAS INFORMAÇÕES

5.20- Todos os direitos autorais dos materiais fornecidos com base neste termo são de propriedade da CONTRATADA, sendo expressamente vedada sua reprodução e divulgação;

5.21- A CONTRATADA e todos os funcionários envolvidos no processo de contratação e execução das atividades deverão manter sigilo absoluto sobre quaisquer informações da CONTRATANTE;

5.22- É proibida a interceptação de qualquer tráfego oriundo ou destinado à CONTRATANTE sem autorização judicial.

6. MODELO DE GESTÃO DO CONTRATO

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

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

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

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

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

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

Fiscalização

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

Do fiscal do contrato

6.7. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

6.8. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

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

6.10. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

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

6.12. O gestor do contrato comunicará, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

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

6.14. Caso ocorra descumprimento das obrigações contratuais, o fiscal do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

Gestor do Contrato

6.15. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

6.16. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

6.17. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

6.18. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

6.19. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

6.20. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

Sanções

6.21. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

a) dar causa à inexecução parcial do contrato;
b) dar causa à inexecução parcial do contrato que cause grave dano à administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) dar causa à inexecução total do contrato;
d) deixar de entregar a documentação exigida;
e) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
f) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
g) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
h) apresentar declaração ou documentação falsa ou prestar declaração falsa durante a licitação ou a execução do contrato;

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

i) fraudar a licitação ou praticar ato fraudulento na execução do contrato;
j) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
k) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
l) praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, de 1º de agosto de 2013.

6.21.1. Constituem comportamentos que serão enquadrados na letra d, do item 8.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou da execução contratual:

a) deixar de entregar documentação exigida no instrumento convocatório;
b) entregar documentação em manifesta desconformidade com as exigências do instrumento convocatório;
c) fazer entrega parcial de documentação exigida no instrumento convocatório;
d) deixar de entregar documentação complementar exigida pelo Agente de contratação ou Pregoeiro, necessária para a comprovação de veracidade e/ou autenticidade de documentação exigida no edital de licitação.
e) deixar de atender a convocações do Agente de Contratação ou pregoeiro durante o trâmite do certame ou atendê-las de forma insatisfatória.

6.21.2. Constituem comportamentos que serão enquadrados na letra e do item 8.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou da execução contratual:

a) não enviar a proposta adequado ao último lance ofertado ou após a negociação;
b) deixar de encaminhar ou encaminhar em manifesta desconformidade com o instrumento convocatório as amostras solicitadas pelo Agente de Contratação ou Pregoeiro;
c) ofertar preço inexequível na formulação da proposta inicial ou na fase de lances;
d) recusar-se a enviar o detalhamento da proposta quando exigível;
e) solicitar a desclassificação após a abertura da sessão do certame;
f) abandonar o certame.

6.21.3. Constituem comportamentos que serão enquadrados na letra f do item 8.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou execução contratual:

a) recursar-se a assinar o contrato ou a ata de registro de preço;
b) recusar-se a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração.

6.21.4. Constituem comportamentos que serão enquadrados na letra j do item 8.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou execução contratual, a prática de quaisquer atos direcionados a prejudicar o bom andamento do certame ou do contrato, em especial:

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

a) agir em concluiu ou em desconformidade com a lei;
b) induzir deliberadamente a erro no julgamento;
c) apresentar amostra falsificada ou deteriorada.

6.22. O licitante ou contratado que incorra nas infrações previstas, garantido o contraditório e a ampla defesa, sujeitar-se-ão às seguintes sanções:

a) advertência;
b) multa;
c) impedimento de licitar e contratar;
d) declaração de inidoneidade para licitar ou contratar.

6.22.1. A aplicação das sanções acima previstas não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

6.22.2. A sanção de advertência será aplicável nas hipóteses de inexecução parcial do contrato que não implique em prejuízo ou dano à administração, bem como na hipótese de descumprimento de pequena relevância praticado pelo licitante ou fornecedor e que não justifique imposição de penalidade mais grave.

6.22.3. A sanção de multa terá natureza moratória ou compensatória e poderá ser aplicada isolada ou cumulativamente com as demais sanções acima previstas, no caso de cometimento de qualquer das infrações administrativas previstas no item 8.1.

6.22.3.1. A multa moratória será aplicada nas hipóteses de atraso injustificado na execução do contrato.

6.22.3.2. A multa compensatória será aplicada nas hipóteses de descumprimento de obrigações contratuais, sendo estabelecidas em razão do grau de importância da obrigação desatendida, objetivando-se a compensação das eventuais perdas nas quais a Administração tenha incorrido.

6.22.3.3. A multa moratória será de 0,5% (cinco décimos por cento) por dia de atraso na entrega de material ou execução do serviço, recaindo o cálculo sobre o valor da parcela inadimplida até o limite de 30% (trinta por cento) do contrato ou do instrumento equivalente.

6.22.3.4. A aplicação de multa de mora não impedirá que a administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções acima previstas.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

6.22.3.5. Poderá ser aplicada multa compensatória de até 3% (três por cento) sobre o valor de referência ao licitante ou contratado que retardar o procedimento de contratação, descumprir preceito normativo ou obrigações assumidas, tais como:

a) tumultuar a sessão pública da licitação;
b) propor recursos manifestamente protelatórios em sede de contratação direta ou de licitação;
c) deixar de providenciar o cadastramento da empresa vencedora da licitação ou da contratação direta junto ao Sistema de Cadastro de Fornecedores dentro do prazo concedido, salvo por motivo justificado e aceito pela administração;
d) deixar de cumprir as exigências de reserva de cargos previstas em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz;
e) deixar de cumprir o modelo de gestão do contrato;
f) deixar de complementar o valor da garantia recolhida após solicitação do contratante;
g) não devolver os valores pagos indevidamente pelo contratante;
h) não manter, durante a execução do contrato, todas as condições exigidas para a habilitação, em caso de licitação, ou para a qualificação, em caso de contratação direta, ou, ainda, quaisquer outras obrigações;
i) deixar de regularizar, no prazo definido pela administração, os documentos exigidos pela legislação para fins de liquidação e pagamento da despesa;
j) manter funcionário sem qualificação para a execução do objeto;
k) utilizar as dependências do contratante para fins diversos do objeto do contrato;
l) deixar de substituir empregado cujo comportamento for incompatível com o interesse público, em especial quando solicitado pela administração;
m) deixar de efetuar o pagamento de salários, vale-transporte, vale-refeição, seguros, encargos fiscais e sociais, bem como deixar de arcar com quaisquer outras despesas relacionadas à execução do contrato nas datas avençadas;
n) deixar de apresentar, quando solicitado, documentação fiscal, trabalhista e previdenciária regularizada;
o) deixar de regularizar os documentos fiscais no prazo concedido na hipótese de o licitante ou contratado enquadrar-se como Microempresa, Empresa de Pequeno Porte ou equiparados, nos termos da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;
p) não manter atualizado e-mail para contato, sobretudo dos prepostos, nem informar à gestão e à fiscalização do contrato, no prazo de dois dias úteis, a alteração de endereços, sobretudo quando este ato frustrar a regular notificação de instauração de processo sancionador;
q) subcontratar o objeto ou a execução de serviços em percentual superior ao permitido no edital ou contrato, ou de forma que configure inexistência de condições reais de prestação do serviço ou fornecimento do bem.

6.22.3.6. Poderá ser aplicada multa compensatória de até 5% (cinco por cento) sobre o valor da parcela inadimplida ao licitante ou contratado que entregar o objeto contratual em

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

desacordo com as especificações, condições e qualidade contratadas ou com irregularidades ou defeitos ocultos que o tornem impróprio para o fim a que se destina.

6.22.3.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela administração ao contratado, além da perda desse valor, a diferença poderá ser paga diretamente à administração, descontada da garantia prestada ou cobrada judicialmente.

6.22.3.8. A multa inadimplida poderá ser descontada de pagamento eventualmente devido pela contratante decorrente de outros contratos firmados com a administração municipal.

6.23. A sanção de impedimento de licitar e contratar com a Administração Pública Municipal será aplicada pelo prazo máximo de três anos, quando não se justificar a imposição de penalidade mais grave, observando-se os parâmetros estabelecidos, aos responsáveis pelas seguintes infrações:

a) dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo: impedimento pelo período de até dois anos;
b) dar causa à inexecução total do contrato: impedimento pelo período de até três anos;
c) deixar de entregar a documentação exigida para o certame: impedimento pelo período de até dois meses;
d) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado: impedimento pelo período de até quatro meses;
e) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta: impedimento pelo período de até seis meses;
f) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado; impedimento pelo período de até um ano.

6.23.1. A aplicação de três sanções de advertência pelo mesmo motivo, em um mesmo contrato, possibilita a aplicação da sanção de impedimento de licitar e contratar.

6.23.2. Será aplicada a sanção de declaração de inidoneidade para licitar e contratar com a Administração Pública direta e indireta, de todos os entes federativos, pelo prazo mínimo de três anos e máximo de seis anos, observando-se os parâmetros estabelecidos, aos responsáveis pelas seguintes infrações:

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

a) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato: até quatro anos;
b) fraudar a licitação ou praticar ato fraudulento na execução do contrato; até seis anos;
c) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; até seis anos;
d) praticar atos ilícitos com vistas a frustrar os objetivos da licitação: até cinco anos;

praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, de 1º de agosto de 2013: até seis anos.

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento

7.1. Os bens serão recebidos provisoriamente, no prazo de 05 (cinco) dias, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 03 (três) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá no prazo de até 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 10 (dez) dias úteis.

7.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.6. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.7. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

liquidação de despesa, não será computado para os fins do recebimento definitivo.

7.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.

7.9. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

7.10. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.11. A Administração deverá realizar consulta para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

7.12. Constatando-se a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.13. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.14. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.15. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação.

Prazo de pagamento

7.16. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior.

7.17. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

Forma de pagamento

7.18. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

7.20. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.20.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

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

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Forma de seleção e critério de julgamento da proposta

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

Forma de fornecimento

8.2. O fornecimento do objeto será parcelado para o item 06 e integral para os demais itens deste termo de referência.

Exigências de habilitação

8.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

8.4. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede; ou

8.5. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor; ou

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

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

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

Habilitação fiscal, social e trabalhista

8.8. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

8.9. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.10. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.11. Prova de regularidade perante a Justiça do Trabalho;

8.12. Prova de inscrição no cadastro de contribuintes Estadual ou Municipal, se houver, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.13. Prova de regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do fornecedor;

8.14. Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

Qualificação Econômico-Financeira

8.15. Não exigida.

Qualificação Técnica

8.16. Não exigida.

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

O custo total da contratação é de R$ 195.487,27 (cento e noventa e cinco mil, quatrocentos e oitenta e sete reais e vinte e sete centavos), conforme custos unitários apostos na tabela anexa ao ETP.

9.1. Justificativa do preço: a estimativa de preços se deu mediante comprovação dos preços praticados de outras administrações por consulta em sites e por de consultas a prestadores de serviço, conforme mapa de preços em anexo.

10. ADEQUAÇÃO ORÇAMENTÁRIA

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

Itabirito, 20 de dezembro de 2024.

_____

Layane Cristine Faria Andrews
Chefe de Departamento Administrativo

_____

Filipe Augusto Serra Palheiros
Chefe de TI

Av. Queiroz Júnior, nº 639, Praia - Itabirito/MG - CEP: 35.450-228
Telefone: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Estudo Técnico Preliminar 20/2024

1. Informações Básicas

Número do processo: 465/2024

2. Descrição da necessidade

Com os avanços tecnológicos, surgiram também ameaças cibernéticas, as quais impõem aos usuários da internet e da ethernet a necessidade de protegerem suas redes e seus dados de ameaças, tais como malware como ransomware e phishing. Os órgãos públicos são grandes armazenadores de dados, além de causarem grande prejuízo à população quando interrompem seus serviços, o que os tornam alvos de diversas formas de ataques cibernéticos e com diferentes possibilidades de danos.

A sede da Câmara de Itabirito hoje possui o software pfSense como solução de Firewall (sistema de segurança de rede). Apesar da vantagem deste sistema ser open source, ele não garante atualizações constantes nem a continuidade do serviço. Constantemente o Departamento de TI depara com o fato desta versão gratuita não atender as necessidades de controle e gerenciamento da rede. Há outros agravantes referentes a utilização deste software como, a necessidade de instalar e configurar diversos pacotes e plugins que não são nativos do sistema. Estas parametrizações são em sua maioria das vezes complexas de serem feitas. Por exemplo, a instalação e manutenção dos módulos de monitoramento das atividades dos usuários, recursos para limitações de largura de banda, serviços de VPN, filtros de conteúdo e regras para detecção e prevenção de intrusão.

Além do mais, o servidor que hospeda o firewall pFSene é um computador genérico e convencional que possui um hardware insuficiente para atender o throughput exigido pela rede, ou seja, é um equipamento inadequado para ser utilizado para processar os pacotes que trafegam entre todos os dispositivos conectados e a internet.

O Centro de Atendimento ao Cidadão (CAC), o anexo da Câmara e os gabinetes dos vereadores não possuem um sistema de firewall implantado em suas respectivas redes que são independentes. Portanto, há uma carência nestes locais de um sistema que funcione como uma barreira de proteção contra invasões, ataques externos, guarda dos dados sensíveis, filtro de acessos e bloqueio de navegações suspeitas.

Outra necessidade é a adequação e preparação da estrutura do ambiente para comunicação junto a unidades externas, permitindo a unificação das redes da Câmara por meio de tecnologias como VPN, FTP, MPLS, VLAN. Esta opção irá facilitar o compartilhamento de arquivos entre os colaboradores e agilizar na comunicação por meio de ferramentas internas de produtividade, resultando na economia de recursos computacionais e centralizando todo o gerenciamento de acesso.

A modernização do ambiente computacional para acessibilidade dos equipamentos corporativos e não corporativos por meio da topologia sem fio se tornou imprescindível. Atualmente são utilizados pela Câmara access points tradicionais que não são recomendados para ambientes institucionais por não possuírem níveis de segurança desejáveis, alto desempenho, confiabilidade, gerenciamento e recursos avançados de autenticação.

Os usuários dos gabinetes dos vereadores são desprovidos de conexão de acesso sem fio para dispositivos móveis e frequentemente estes colaboradores informam ao departamento de TI sobre a necessidade deste tipo de acesso. Ainda não foi disponibilizado este tipo de conexão devido a Câmara não possuir equipamento adequado para operar neste ambiente. Os access points tradicionais que temos não são compatíveis com o espaço em razão do alto número de usuários, área interna extensa e necessidade de um sistema de autenticação para atender a segurança da informação e aplicação da LGPD.

Outro agravante é o fato do sinal de telefone nesta região ser de baixa qualidade, diversas vezes não funciona, e cai constantemente deixando os colaboradores com uma comunicação precária por meio dos dispositivos móveis.

Portanto além do Firewall, há a necessidade de aquisição de equipamentos Access Point profissionais para promover a interconexão da rede cabeada com as diversas redes wireless da sede da Câmara, CAC, Anexo e gabinetes dos vereadores, uma vez que os dispositivos existentes na Câmara são inadequados.

Deste modo, esta contratação reflete uma necessidade evidente por recursos tecnológicos essenciais aos objetivos da Câmara de Itabirito, como medida eficaz, integrada, de ampliação e manutenção capaz de absorver as demandas, sempre crescentes, de capacidade, desempenho e disponibilidade, internas e externas, sem comprometer o resultado da prestação de serviços públicos.

Dado o exposto, faz-se necessária a contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall (destinado à proteção da rede) e access point (destinado a acessibilidade segura sem fio), para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara Municipal de Itabirito, uma vez que é de interesse público que a Câmara possua suas redes seguras e maior acessibilidade por meio de conexão sem fio, com qualidade, segurança e com garantia de não interrupção dos serviços, para o bom desempenho de suas atribuições.

O quantitativo de equipamentos e demais objetos a serem contratados para suprirem a demanda foram estabelecidos mediante análise da equipe do Departamento de Tecnologia da Informação, descrita neste estudo.

Os objetos desta contratação são caracterizados como bens comuns, por possuírem sua qualidade e desempenho definidos por padrões de mercado. Assim sendo, os bens se enquadram no art. 6° inciso XIII da Lei 14.133 de 2021.

O objeto da contratação está previsto no Plano de Contratações Anual 2023.

3. Área requisitante

Área Requisitante	Responsável
Diretoria Administrativa	André Luiz Almeida de Souza

4. Necessidades de Negócio

O contrato deverá permitir maior acessibilidade e segurança a rede da Câmara Municipal de Itabirito e deve seguir os seguintes requisitos:

O contrato deverá atender toda a demanda da Câmara Municipal de Itabirito;

Fornecer equipamentos hardware e software;

Fornecer pacotes de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web pelo prazo de 36 (trinta e seis) meses;

Fornecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. Deve funcionar em conjunto com o equipamento de firewall;

Fornecimento prestação de serviços para instalação, configuração e ativação da solução;

Fornecer suporte técnico do fabricante para o hardware com garantia da solução;

Fornecer licenciamento do software para atualizações;

Fornecimento de repasse tecnológico através de treinamento para a correta utilização dos equipamentos de hardware e dos softwares.

A CONTRATADA deverá realizar os serviços de instalação e configuração dos equipamentos e licenciamentos de forma a garantir o seu pleno funcionamento no ambiente tecnológico da Câmara de Itabirito.

O planejamento, instalação, configuração e ativação dos equipamentos deverão ser executados por profissionais qualificados e a empresa deverá ser credenciada pelo fabricante dos equipamentos.

A CONTRATADA deverá garantir todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue.

Todas as configurações serão realizadas em conformidade com a recomendação do fabricante dos equipamentos e softwares da solução existente, boas práticas de implementação recomendada pelo fabricante e os requisitos fornecidos pela Câmara de Itabirito ao ambiente em questão.

Todos os equipamentos adquiridos na solução deverão ser instalados, configurados, testados e integrados na estrutura existente (rede de dados) da Câmara de Itabirito, garantindo assim a total compatibilidade e interoperabilidade de sua infraestrutura.

A CONTRATADA deverá realizar as transferências de regras e migrações de parâmetros existentes nos firewalls atuais mediante disponibilização de acesso e acompanhamento técnico da contratante. Os equipamentos firewalls utilizados atualmente no ambiente da contratante são: 1 servidor físico pfSense e 1 Routerboard Mikrotik RB750Gr3, ambos utilizados em topologia bastion host (o firewall está localizado entre a internet e o segmento de rede interna).

Os equipamentos e serviços serão aceitos mediante comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos e a solução se encontre em operação plena. Essa comprovação será realizada por meio de observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações.

A CONTRATADA deverá fornecer catálogos, manuais e/ou prospectos (em formato físico ou digital) de todos os materiais e equipamentos entregues.

Na execução do serviço, deve estar incluída pela CONTRATADA toda mão de obra necessária para instalação física e configuração dos equipamentos para o funcionamento pleno dos Access Point.

Deve ser realizado pela CONTRATADA toda a estrutura de cabeamento de redes de dados para interligação entre a área de instalação do Access Point e o backbone da Câmara de Itabirito.

A CONTRATADA, se necessário, deverá prover a instalação de pontos de elétrica para a interligação do access point até o quadro de distribuição de energia existente na estrutura da Câmara de Itabirito.

Deve ser fornecido pela CONTRATADA, caso necessário, material para a instalação dos Access Point como buchas, parafusos, conectores, eletrodutos, conduletes, canaletas, tomadas, cabos, caixas sistema x, tampas, espelhos e suportes.

Deve ser providenciado pela contratada qualquer eventual serviço necessário para execução da instalação física dos Access Point como, por exemplo, furos e reparos em alvenarias ou gessos.

Deve incluir a fixação de equipamentos e materiais com o devido acabamento necessário em conformidade com a arquitetura presente no ambiente.

A contratante irá disponibilizar espaço no rack / armário para abrigar o equipamento Hardware Firewall. Caso não haja espaço será fornecido um novo rack / armário pela contratante para ser instalado pela contratada.

Caberá, portanto, à CONTRATADA a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos.

A CONTRATADA deverá designar um profissional Técnico Responsável para acompanhar a execução dos serviços desde o planejamento até a implantação da solução.

Após as fases de implantação dos equipamentos, a equipe técnica da CONTRATADA deverá realizar a transferência tecnológica da solução à equipe técnica da Câmara de Itabirito.

A CONTRATADA deve realizar o teste de funcionamento dos equipamentos, após sua instalação, na presença do contratante.

Todos os serviços de instalação, configuração e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

Durante os primeiros 2 (dois) dias úteis após a instalação e ativação do sistema, a CONTRATADA deverá manter, no mínimo, 01 (um) técnico para a operação assistida e fornecimento de suporte, nas dependências da Câmara de Itabirito, sem custo adicional para a Autarquia.

Caberá à CONTRATADA a realização dos demais serviços necessários ao pleno funcionamento da solução fornecida.

Adicionalmente a CONTRATADA deverá:

- Planejar a instalação e implantação da solução e elaborar o cronograma;
- Instalar os equipamentos de acordo com a proposta de hardware deste termo;
- Implantar o firewall de nova geração, migrar as configurações existentes para o mesmo e vincular ao AD;
- Integrar o firewall aos endpoints;
- Instalação física e lógica;
- Instalar Cabling e alimentação elétrica dos ativos;
- Configuração de regras, a serem definidas com o time;
- Validações de regras;
- Entregar a documentação pertinente: relatório conclusivo com as configurações e parâmetros definidos bem como um resumo de toda a implementação.

Os serviços deverão ser realizados no prazo máximo de 15 (quinze) dias úteis após a data da entrega dos equipamentos.

Realizar o acompanhamento, suporte, e assistência técnica pós instalação por 12 meses, contemplando ajustes de configurações, dúvidas, recuperação de desastres e novas instalações.

Da garantia

A garantia dos equipamentos fornecidos deverá ser realizada pelo fabricante pelo prazo de 03 (três) anos, com assistência técnica e solução no prazo máximo de 06 (seis) horas, comprovados através de declaração do fabricante a garantia ofertada;

A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

Condições de prestação de serviços

A Contratada deverá seguir rigorosamente as normas e padrões estabelecidos, bem como diligenciar para que a prestação de serviço seja feita em perfeitas condições, não podendo conter quaisquer vícios.

A contratada deverá arcar com todos os custos diretos e indiretos oriundos do serviço, incluindo, instalação dos equipamentos, licenças de software, transporte, repasse tecnológico através de treinamento.

A justificativa de quaisquer atrasos no cumprimento de prazos somente será considerada se apresentada por escrito, e após aprovação da Câmara Municipal de Itabirito.

A tolerância com qualquer atraso ou inadimplemento por parte da contratada não importará, de forma alguma, em alteração contratual ou renovação, podendo a solicitante exercer seus direitos a qualquer tempo.

A contratada deverá ser responsável pelo pagamento de todos os encargos, tributos, frete e quaisquer outras contribuições que sejam exigidas para a execução dos serviços.

A contratada assumirá inteira responsabilidade pelas obrigações decorrentes da legislação trabalhista, previdenciária de acidentes de trabalho e quaisquer outras relativas a danos a terceiros.

Dos equipamentos

Os equipamentos deverão atender às quantidades e configurações mínimas do termo de referência e deverão ser novos.

Os equipamentos deverão chegar embalados em caixas dos próprios fabricantes comprovando que são novos, nunca foram utilizados e estão em perfeitas condições de uso.

Sempre que necessário a troca definitiva dos equipamentos devido a defeitos de fabricação, problemas, falhas técnicas e manutenção corretiva a reposição deverá ser feita por equipamentos novos equivalentes ou superiores aos que foram instalados na primeira instalação. A contratada terá o prazo de 24 (vinte e quatro) horas para a entrega de suprimentos, contados da solicitação da Câmara ou detecção pelo sistema de monitoramento de nível de suprimentos. As despesas com fretes, transportes de equipamentos e materiais, assim como a descarga e a movimentação dos mesmos até os locais de instalação, bem como, deslocamento de funcionários e equipe técnica, serão de responsabilidade exclusiva da CONTRATADA.

Da assistência técnica

A assistência técnica dos equipamentos deverá ser executada pelo fabricante ou empresa credenciada pelo mesmo, comprovado através de declaração do fabricante assumindo a assistência técnica durante a garantia e, no caso, de execução por parte de empresa credenciada, indicar a empresa com os correspondentes contatos.

Serviço de suporte técnico

Serviço de suporte técnico deve ser prestado pela contratada. Este serviço se difere da assistência técnica de hardware do fabricante e garantia que estão incluídos na subscrição dos equipamentos.

Durante o período de suporte técnico, a CONTRATANTE poderá solicitar o suporte técnico remoto ou presencial especializado a contratada, com limite de 4 (quatro) visitas presenciais por mês;

A solicitação de suporte técnico por parte da contratada se dará através de abertura de chamado, a ser realizado por, no mínimo, os seguintes meios de comunicação, disponibilizados sempre em idioma português (Brasil): ligação telefônica, sistema web (website) com autenticação segura (mínimo usuário e senha de acesso), e-mail corporativo (em caso de indisponibilidade dos meios anteriormente citados);

O suporte técnico deverá estar disponível na modalidade “5x7” (2ª à 6ª, horário comercial);

A CONTRATADA deverá realizar mensalmente manutenções preventivas, inspeções e conferência dos parâmetros dos equipamentos de forma a garantir o pleno funcionamento e assegurar que as configurações de segurança estejam sendo aplicadas conforme critérios definidos durante a implantação.

O suporte deverá respeitar, no mínimo, os seguintes tempos de resposta para os níveis de severidade abaixo:

- Crítica: solução inoperante ou falha de grande impacto causando parada na solução - Atendimento em até 2 (duas) horas, com solução em até 6 (seis) horas;
- Alta: incidentes que causem danos moderados à solução, como lentidão elevada, travamentos, interrupções recorrentes - Atendimento em até 4 (quatro) horas, com solução em até 8 (oito) horas;
- Baixa ou informativa: incidentes de baixo impacto, como lentidão esporádica, erros em ferramenta de geração de relatórios. Inclui também chamados para esclarecimento de dúvidas sobre a configuração e/ou funcionamento da solução - Para este nível de severidade o tempo de resposta deverá ser de até 2 (dois) dias, em horário comercial.

O serviço de suporte técnico deverá ser realizado pelo período de 12 meses, que será contado após a validação pela contratante da entrega dos serviços de instalação (item 4) e serviço de treinamento (item 5) pela contratada.

O serviço de suporte técnico será pago de forma mensal pela contratante sendo dividido por 12 parcelas do valor total proposta pela contratada.

Os serviços de suporte técnico deverão ser executados por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

Serviço de treinamento

Deverá ser realizado programa de treinamento, de forma a capacitar os profissionais da Câmara de Itabirito na utilização dos equipamentos e softwares envolvidos na solução ofertada.

A contratada deve realizar treinamento com transferência de conhecimento para no mínimo 2 pessoas com no mínimo de 32 horas (incluídos nessas horas as 16 horas de implantação assistida).

O treinamento deverá abranger todos os equipamentos, componentes e softwares da solução ofertada, em seus aspectos mais relevantes como instalação, configuração e gerenciamento, tomando por base a Documentação do Projeto, e ainda contemplando princípios básicos de funcionamento, noções de manuseio, operação e conservação, principais comandos e procedimentos diários de operação, procedimentos de emergência a serem executados em casos de contingência, geração, emissão e análise de relatórios.

A CONTRATADA fornecerá treinamento aos colaboradores da CONTRATANTE, com instrutor certificado pelo fabricante, buscando garantir a utilização de práticas corretas na operação do ambiente e a correta reação nos casos de incidentes envolvendo os sistemas do Data Center.

O escopo do plano de treinamento para instalação, operação e configuração, gerenciamento centralizado e gerenciamento de relatórios deve prever:

- Informativo global dos componentes tecnológicos envolvidos na prestação dos serviços contratados;

- Compreensão geral da filosofia de funcionamento e de operação;
- Conhecimento e usabilidade dos recursos (hardwares e softwares) envolvidos;

Funcionalidades do Sistema em seus respectivos módulos;

Reinstalação, implantação e configuração dos equipamentos de Firewall e Access Point;

Parametrização, criação de regras, backups, gerenciamento dos equipamentos de Firewall e Access Point;

Gerenciamento, monitoramento e emissão de relatórios e logs da solução do objeto da contratação.

O treinamento deverá ser ministrado em local, data e horário indicado pela CONTRATANTE, de modo que o aluno possa praticar, ao menos, a configuração, o gerenciamento e a operação dos equipamentos, soluções e softwares que compõem o data center;

A capacitação na solução deverá acontecer no prazo máximo de 30 (trinta) dias após a instalação e configuração dos equipamentos, no local de instalação dos equipamentos.

Todos os serviços de treinamento e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

Sigilo e propriedade das informações

Todos os direitos autorais dos materiais fornecidos com base neste termo são de propriedade da CONTRATADA, sendo expressamente vedada sua reprodução e divulgação;

A CONTRATADA e todos os funcionários envolvidos no processo de contratação e execução das atividades deverão manter sigilo absoluto sobre quaisquer informações da CONTRATANTE;

É proibida a interceptação de qualquer tráfego oriundo ou destinado à CONTRATANTE sem autorização judicial.

5. Necessidades Tecnológicas

Característica geral dos equipamentos:

Os equipamentos fornecidos deverão estar em conformidade com programas de redução de consumo de energia.

Descrição de solução de segurança de rede – NGFW (item 1)

Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.

Dispositivo remoto de ethernet, para oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos.

Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / malwares, assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período mínimo de 36 (trinta e seis) meses.

Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.

Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento.

Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).

Por alta disponibilidade (HA) entende-se que a solução deverá ser composta ao menos por dois appliances, licenciados para funcionamento em redundância.

A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um equipamento (sempre em modo de alta disponibilidade HA) para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.

Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

Descrição e características de firewall (NGFW) ou dispositivo remoto de ethernet

Deve ser do mesmo fabricante do firewall e em forma de appliance.

Deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso aos recursos remotos.

O túnel seguro deve ter no mínimo 850 Mbps de throughput utilizando criptografia AES256 e TLS 1.2.

Deve suportar módulo adicional de Wi-fi MIMO 2x2:2, com rádio padrão mínimo 802.11 a/b/g/n/ac Wave 1 (Wi-Fi 5), habilitado para banda dupla ou 4G/LTE.

Deve possuir no mínimo 04(quatro) interfaces 10/100/1000 Base-TX (1 GbE de cobre).

Deve possuir no mínimo 02(duas) interfaces USB 3.0. Possuir luzes indicativas no mínimo equipamento ligado, interface de rede ligada.

Possuir fonte de alimentação bivolt compatível com 110-240 V, 50-60 Hz. (RED15/REDE15w).

Deve suportar uma 2ª fonte de alimentação.

Possuir no mínimo as certificações CE/FCC/IC/RCM/VCCI/CB/UL/CCC/KC/ANATEL.

Operar com umidade de no mínimo entre 10% a 90%, sem condensação.

Deve ser possível ser gerenciado pelo equipamento concentrador.

Deve ser possível pelo equipamento concentrador atualizar todos os firmwares de forma a facilitar a manutenção.

Deve permitir carregar a configuração por USB ou de forma automática.

Uplink deve permitir a configuração estática de IP ou através de DHCP.

Deve possuir a funcionalidade de gerenciar o DHCP de forma centralizada.

Deve possuir alta disponibilidade implementando fail-over nos túneis com a matriz.

Deve possuir a funcionalidade de balanceamento entre dois túneis com a matriz.

Para facilitar a implementação de regras específicas por regiões deve aparecer como interface no concentrador central.

Para facilitar a implementação de regras específicas deve possuir funcionalidade de agregar logicamente todas as localidades como uma interface no concentrador central.

Deve ter a funcionalidade de compressão do túnel de forma a otimizar a banda utilizada.

Deve possuir a funcionalidade de filtrar por MAC.

Características específicas de desempenho e hardware do firewall de próxima geração - NGFW

Performance mínima de 10.500 Mbps de throughput para firewall.

Performance mínima de 2.500 Mbps de throughput para firewall NGFW.

Performance mínima de 3.250 Mbps de throughput de IPS.

Performance mínima de 900 Mbps de throughput para controle de AV/proxy.

Performance mínima de 1.800 Mbps de throughput de VPN.

Suporte a, no mínimo, 5.000.000 (5 milhões) de conexões simultâneas.

Suporte a, no mínimo, 69.900 (sessenta e nove mil e novecentos) novas conexões por segundo.

Possuir o número irrestrito quanto ao máximo de usuários licenciados.

Possuir armazenamento interno de no mínimo 64 GB SSD para sistema operacional, quarentena local, logs e relatórios.

Possuir no mínimo 4GB de memória RAM.

Possuir no mínimo 12 (doze) interfaces de rede GbE1000Base-TX.

Possuir no mínimo 2 (duas) interfaces SFP Fiber.

Possuir no mínimo 1 (um) módulo de expansão de interfaces.

Possuir 1 (uma) interface do tipo console ou similar.

Características gerais para firewalls de próxima geração

O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), console de gerência, monitoração e logs.

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários, controle granular de permissões, IPS, Firewall, Antispam, VPN IPSec, SSL VPN e SSL Inspection.

As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica.

Todos os equipamentos fornecidos poderão ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação.

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

O software deverá ser fornecido em sua versão mais atualizada.

A solução deverá ter capacidade de operar em alta Disponibilidade (HA). O HA deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.

Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.

A atualização de software deverá enviar avisos de atualização automáticos.

O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

As notificações deverão ser realizadas via e-mail e SNMP.

Suportar SNMPv3 e Netflow.

O firewall deverá ser stateful, com inspeção profunda de pacotes.

As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

As políticas de NAT deverão ser customizáveis para cada regra.

A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS).

Proteção contra anti-spoofing.

Suportar IPv4 e IPv6.

IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).

Deve possuir tecnologia de conectividade SD-WAN;

A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN;

Deve implementar balanceamento entre os links WAN com método SpillOver;

Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN;

Deve suportar o uso de, no mínimo, 3 (três) links;

Deve suportar o uso de links de interfaces físicas, subinterfaces lógicas de VLAN e túneis IPSec;

Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde;

A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima;

Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês;

A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado;

A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador;

Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;

A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados;

Deve possibilitar o roteamento baseado em VPNs;

Deve suportar criar políticas de roteamento;

Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:

- Interface de entrada do pacote;
- IPs de origem;
- IPs de destino;
- Portas de destino;
- Usuários ou grupos de usuários;
- Aplicação em camada 7.

Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento;

Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

Deve suportar Extended VLAN;

O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.

A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

Deve permitir a configuração de jumbo frames nas interfaces de rede;

Deve permitir a criação de um grupo de portas layer2;

A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal;

A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;

O traffic shapping (QoS) deverá ser baseado em rede ou usuário.

A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

Deve possuir otimização em tempo real de voz sobre IP.

Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

Controle por políticas de firewall

Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

Controle de políticas por países via localização por IP.

Suporte a objetos e regras IPV6.

Suporte a objetos e regras multicast.

Prevenção de ameaças

Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, Anti-Malware e Firewall de Proteção Web (WAF) integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes politicas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;

A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em núvem;

Para a eficácia da análise de malwares Zero-Days, a solução de Sandobox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning;

A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma;

Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em núvem;

A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-e-mails.

A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.

Deve ter proteção em tempo real contra novas ameaças criadas.

Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.

Deve permitir o bloqueio de vulnerabilidades.

Deve permitir o bloqueio de exploits conhecidos.

Deve detectar e bloquear o tráfego de rede que busque acesso a command and control e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.

Deve incluir proteção contra-ataques de negação de serviços.

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

Suportar bloqueio de arquivos por tipo.

Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

Os eventos devem identificar o país de onde partiu a ameaça.

Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.

O equipamento do tipo 1 deve ter a capacidade de atuar como um gateway AntiSpam de modo que possa realizar filtragens dos e-mails e aplicar políticas.

O gateway de e-mail incluso no equipamento do tipo 1 deve ter pelo menos as seguintes proteções:

- Sender Policy Framework (SPF);
- Domain Keys Identified Mail (DKIM);
- Domain-based Message Authentication, Reporting & Conformance (DMARC);
- Bounce Address Tag Validation (BATV);
- O filtro de e-mail deve quarentenar os e-mails suspeitos ou realmente maliciosos;

A solução deve possibilitar aos usuários acessarem um painel para verificação da sua caixa pessoal de quarentena, possibilitando então a liberação ou a exclusão das mensagens;

A função de AntiSpam deve permitir a configuração de relays com a possibilidade de autenticação deles;

A função de AntiSpam deve possibilitar também o envio de e-mails seguros, realizando a criptografia das mensagens bem como dos seus anexos.

A função de AntiSpam deve conter funcionalidades de prevenção a perda de dados (DLP) para evitar que informações sigilosas sejam vazadas;

O equipamento deverá possuir firewall de aplicação Web (WAF) com a função de reverse proxy, função de URL hardening realizando deep-linking e prevenção dos ataques de path traversal ou directory traversal.

O firewall de aplicação Web (WAF) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.

O firewall de aplicação Web (WAF) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do WAF e permissão e bloqueio de ranges de IP.

Deverá permitir a identificação dos IPs de origem através de proxy via “X-forward headers”.

Deve possuir pelo menos duas engines de antivírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.

Proteção pelo menos contra os seguintes ataques, mas não limitado a: SQL injection e Cross-site scripting.

Controle e proteção de aplicações

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.

Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3.

O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas.

Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website).

Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Atualizar a base de assinaturas de aplicações automaticamente.

Reconhecer aplicações em IPv6.

Limitar a banda usada por aplicações (traffic shaping).

Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuem acesso a estes aplicativos devem ter a utilização bloqueada.

Controle e proteção web

Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Radius, E-directory e base de dados local;

Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius;

Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

Possuir pelo menos 90 categorias de URLs;

Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;

Deve ser capaz de forçar as restrições do Youtube;

Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;

Suportar a criação categorias de URLs customizadas;

Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada.

Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;

Deve realizar caching do conteúdo web;

Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet.

A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual.

A solução deve permitir o enforce dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar.

Identificação de usuários

Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

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

Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, afim de garantir que usuários logados em servidores de multi sessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas um IP de origem;

Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.

Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

Qualidade de serviço – QoS

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bit rate de modo individual ou compartilhado.

Suportar priorização Real-Time de protocolos de voz (VoIP).

Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

Redes virtuais privadas – VPN

Suportar VPN Site-to-Site e Cliente-to-Site.

Suportar IPsec VPN.

Suportar SSL VPN.

Suportar L2TP e PPTP.

Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.

Deve possuir opção de VPN IPSEC com aplicação nativa do fabricante.

Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.

Deve suportar nativamente a integração com a Amazon, a fim de estabelecer um túnel seguro entre os equipamentos e a VPN da AWS.

Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

Suportar autenticação via AD/LDAP, Token e base de usuários local;

Permitir estabelecer um túnel SSL VPN com uma solução de autienticação via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local.

Gerência administrativa centralizada

Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

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

Estar licenciada para gerenciar as soluções de firewall de próxima geração.

Devem ser fornecidas soluções virtuais, em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação.

Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração, sem necessidade de acesso direto aos equipamentos.

Deve permitir a criação de Templates para configurações.

Deve possuir indicadores do estado de equipamentos e rede.

Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas;

Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

Deve possibilitar o envio dos logs via syslog com conexão segura (TLS).

Gerência de logs e relatórios centralizados

Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

Estar licenciada para gerenciar as soluções de firewall de próxima geração.

Devem ser fornecidas soluções virtuais, em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 2TB de dados.

Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

Deve possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

Deve conter relatórios pré configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;

Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

Deve conter customizações dos relatórios para inserção de logotipos próprios.

Deve fornecer relatórios de compliance SOX, HIPAA e PCI.

Deve permitir a exportação via PDF ou Excel.

Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

Deve fornecer relatórios de tendências.

Deve fornecer logs em tempo real, de auditoria e arquivados.

Deve possuir mecanismo de procura de logs arquivados.

Deve ter acesso baseado em Web com controles administrativos distintos.

Integração com solução de endpoint

A solução de firewall deve possibilitar a integração com a atual solução de Endpoint (Sophos Cloud) instalada no ambiente da contratante.

A integração deve possibilitar a criação de regras de bloqueio de endpoints, com determinado status, dentro do Firewall de forma automática, sem que haja intervenção por parte do time da contratante.

A integração deverá ser nativa entre o firewall e o endpoint, ou utilizando APIs de integração da solução de firewall.

Caso a integração não seja nativa, cabe a CONTRATADA:

- Desenvolver completamente a solução de integração do Firewall e o Endpoint instalado (Sophos Cloud);
- O Software de integração deve realizar a criação das regras do Firewall com no máximo 2 (dois) minutos após o incidente detectado no Endpoint;

Possuir interface WEB, acessada por HTTP ou HTTPS, para definição dos objetos das regras a serem criados, com no mínimo origem, destino, status do endpoint e protocolos;

Possibilitar o envio de e-mails sobre as ações do software;

Entregar o software de integração em máquina virtual, Windows ou Linux, juntamente com as devidas licenças necessárias para sistemas operacionais, banco de dados, etc;

A máquina virtual será instalada no ambiente da contratante, não sendo permitido soluções em nuvem;

A máquina virtual não deverá ter qualquer acesso remoto que não seja acordado pela contratante;

A mesma não deverá enviar/receber pacotes TCP/UDP ou por qualquer outro meio de comunicação, que não sejam os objetos de Firewall deste edital ou a console do endpoint da contratante;

A gestão do sistema operacional da máquina virtual em questão será de inteira responsabilidade da contratante, de modo a garantir que sejam realizados todos os updates, correções de patchs, segurança do sistema operacional, bem como com seus softwares, alterações de versões, etc;

A máquina virtual deve ser utilizada única e exclusivamente para o fim proposto no edital, não sendo permitido que a máquina virtual realize qualquer outra função;

Permitir backup das configurações do software de integração, possibilitando o restore em outra máquina virtual de forma a não comprometer o ambiente;

Realizar manutenção/alteração total no software de integração, sem custo adicional, durante o período de vigência do suporte do Firewall Tipo 1;

Realizar teste de bancada, a fim de comprovar a efetividade da integração;

Possuir atendimento 24 horas por dia, 07 dias por semana (24x7), durante todos os dias do ano, inclusive feriados;

O atendimento deve ser realizado por telefone, e-mail, remoto ou on-site (ilimitado);

Apresentar SLA em contrato com os seguintes tempos:

- Criticidade Baixa – Tempo de resposta de até 6 horas e até 48 horas para tempo de solução. Os casos definidos com criticidade baixa são: Falha na console de acesso Web do software de integração, alterações no funcionamento da ferramenta mediante solicitação da contratada, falhas no envio de e-mails por parte do software de integração.
- Criticidade Média - Tempo de resposta de 4 horas e até 8 horas para tempo de solução. Os casos definidos com criticidade média são: Bloqueios inesperados realizados pelo software de integração, falha na identificação do status dos endpoints, falha no job de backup.
- Criticidade Alta – Tempo de resposta de até 2 horas e até 6 horas para tempo de solução. Os casos definidos com criticidade alta são: Sistema operacional da máquina virtual do software de integração inoperante, com problemas durante o boot da VM, qualquer falha no software que comprometa o funcionamento da solução como um todo.

Características específicas do hardware access point (item 3)

Equipamento deve proporcionar o máximo em segurança e desempenho de rede.

Padrão / Normas WLAN: 802.11ax, Wi-Fi 6.

Gerenciamento por meio de plataforma central da fabricante e por interface web local.

Indicado para instalação em ambiente fechado.

Deve permitir ser implantado montado em mesa, parede ou teto.

Rádio duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples.

Deve possuir ao menos 4 antenas omnidirecionais internas, sendo: 2x antenas 2,4 GHz e 2x antenas 5 GHz.

Deve possuir tecnologia DFS (Dynamic Frequency Selection) para gerenciar o uso de frequências de rádio.

Desempenho: 2x 2:2.

Taxas máximas de transmissão: 2975 Mbps sendo 575 Mbps (2,4 GHz) +2400 Mbps (5 GHz).

Interfaces: 1x 12V DC-in, 1x porta Gigabit Ethernet com 802.3at PoE+, Console Micro-USB.

Deve ser ter plataforma na nuvem escalonável que permita o gerenciamento remoto.

Deve possuir recurso de resposta a ameaças ativas para isolamento de hosts comprometidos.

Deve possuir portal cativo para acesso de convidados e visitantes.

Deve permitir o gerenciamento centralizado juntamente com o ecossistema completo das soluções de segurança cibernética da fabricante.

Deve permitir Múltiplos SSIDs.

Deve permitir SSIDs com base em tempo (hora do dia, dia da semana).

Deve permitir Balanceamento de carga do cliente.

Deve permitir Seleção automática de canais.

Deve permitir Seleção de largura do canal.

Deve permitir Direção de banda

Deve permitir Airtime Fairness.

Deve permitir Assistente de roaming (802.11r).

Deve permitir Transição rápida (802.11r).

Deve permitir Portal Cativo: Personalização da página inicial (logotipo, nome, mensagem de boas-vindas, termos e condições).

Deve ser Uniusuário MIMO (SU-MIMO) e Multiusuário MIMO (MU-MIMO).

Deve permitir ter os recursos 802.11 avançados como: Coloração BSS (Basic Service Set), Uplink/Downlink OFDMA e TWT (Target Wake Time).

Deve ter os seguintes recursos de Log e Monitoramento: Captura de Pacotes, Logs de auditoria de Syslog, Log e relatórios de eventos (Relatórios de Syslog), Identidade do usuário (Autenticação baseada no usuário), Detecção de AP ilegítimo.

Deve ter os seguintes recursos de autenticação do usuário / dispositivo: WPA3-Personal SAE, WPA3 Enterprise and Enhanced Open (OWE), Autenticação Enterprise (RADIUS), Filtragem de MAC, Senha diária, semanal, mensal, Autenticação de Backend, Voucher com base em tempo e em cota (de dados), Login via rede social, Isolamento de Cliente, Portal Cativo: Jardim Murado, Rede de convidado – modo de ponte.

Deve ter os seguintes recursos de rede: ARP proxy, Suporte a VLAN, Conversão multicast para unicast, Interface LAG (Link Aggregation Group).

Requisito de energia (PSE) / Potência (máx): 17,5W

Deve ter certificações e conformidades: CB, UL, CE, FCC, ISED, RCM, TEC, EN 60601-1-2 (Diretiva de Equipamentos Médicos).

Deve permitir alimentação elétrica por meio de Power Over Ethernet, padrão 802.3at (Poe +).

O adaptador PoE deve estar incluso como acessório do equipamento.

Padrão PoE mínimo deve ser 30W por porta.

Deve ser fornecido com kit de montagem incluindo: suporte para montagem em parede e teto (barra T de 15/16'' ou 9/16'') e kits para teto plano, plenum e montagem suspensa.

Licenciamento console de controle: Compatível e integrado com o Firewall.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Requisitos Legais

Está em conformidade com a Lei nº 14.133, de 1 de abril de 2021, Lei de normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios.

Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

Requisitos Ambientais, Sociais e Culturais

Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis. Assim como:

- Que causem menor impacto sobre recursos naturais como flora, fauna, ar, solo e água;
- Preferência para materiais, tecnologias e matérias-primas de origem local;
- Maior eficiência na utilização de recursos naturais como água e energia;
- Maior geração de empregos, preferencialmente com mão de obra local;
- Maior vida útil e menor custo de manutenção do bem;
- Uso de inovações que reduzam a pressão sobre recursos naturais;
- Origem ambientalmente regular dos recursos naturais utilizados nos bens e serviços.

Requisitos da implantação da solução

Os equipamentos deverão ser entregues e instalados sem nenhum custo adicional.

Todos os equipamentos deverão ser instalados, configurados e ativados pela CONTRATADA nos locais indicados pela Câmara de Itabirito. Sendo eles:

- Sede da Câmara - Av. Queiroz Junior, nº 639, Bairro Praia, Itabirito/MG.
- Centro de Atendimento ao Cidadão - Rua José Benedito, nº 189 / 3º andar - Bairro Santa Efigênia- Itabirito /MG.

A instalação deverá ser previamente agendada com o gestor do contrato e deverá acontecer em dias úteis no horário de 12:00 às 18:00.

7. Estimativa da demanda - quantidade de bens e serviços

Critérios

Para levantamento dos quantitativos de equipamentos e serviços foram considerados os seguintes critérios:

1. Dimensão das dependências da Câmara Municipal de Itabirito; e

2. Quantitativo de usuários da rede;

3. Além de ter como base os equipamentos já existentes e a necessidade de ampliação e modernização dos mesmos.

Dependências da Câmara Municipal de Itabirito

Atualmente a Câmara Municipal de Itabirito possui suas atividades divididas em duas localidades sendo elas:

- Sede da Câmara Municipal: 426,60 m².
- Anexo da Câmara Municipal: 1.030,72 m².

Tal informação é importante para dimensionar a quantidade de equipamentos necessários para que a rede abranja todo o ambiente da Câmara.

Quantitativo de usuários da rede

A quantidade de usuários da rede possui possíveis variações dada a impossibilidade de uma previsibilidade exata de usuários externos.

- Quantidade estimada de usuários: 120

Equipamentos já existentes

Os equipamentos firewalls utilizados atualmente no ambiente da contratante são: 1 servidor físico pfSense e 1 Routerboard Mikrotik RB750Gr3, ambos utilizados em topologia bastion host (o firewall está localizado entre a internet e o segmento de rede interna). E access points tradicionais que não são recomendados para ambientes institucionais por não possuírem níveis de segurança desejáveis, alto desempenho, confiabilidade, gerenciamento e recursos avançados de autenticação.

O levantamento do Departamento de Tecnologia da Informação, tendo como base os critérios já mencionados anteriormente, bem como a necessidade de ampliação e modernização dos sistemas de firewall e access points constatou a necessidade da aquisição dos seguintes itens:

Equipamentos – Firewall e Access Point **(Lote 1)**				
Itens	Especificação	Quantidade	Valor Unitário	Valor anual

1	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) – Firewall de Próxima Geração – Equipamento com suporte a cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo. Com 03 anos de suporte e garantia de hardware. Pacote de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de Firewall de Próxima Geração (NGFW) pelo prazo de 36 (trinta e seis) meses.	1 (unidade)	R$ 39.680,88	R$ 39.680,88
2	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) ou dispositivo remoto de ethernet – Firewall ou dispositivo deve oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. Deve funcionar em conjunto com o equipamento de firewall (item 01).	1 (unidade)	R$ 15.461,00	R$ 15.461,00
3	Hardware Access Point – Ponto de Acesso Wireless com Rádio Duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples, incluindo adaptador PoE.	8 (unidades)	R$ 7.720,82	R$ 61.766,53
Serviço de instalação, configuração e treinamento (Lote 2)				
Itens	Especificação	Quantidade	Valor Unitário	Valor anual
4	Serviços de instalação, configuração, implantação e migração de regras de Firewall e Access Point.	1 (unidade)	R$ 18.160,83	R$ 18,160,83
5	Treinamento de configuração, gerência e operação do Firewall. A transferência de conhecimento deve ter um total mínimo de 20 horas, feito por profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.	1 (unidade)	R$ 6.200,00	R$ 6.200,00
6	Serviços de suporte e assistência técnica para operação e gerenciamento do Firewall e Access Point.	12 (meses)	R$ 4.518,17	R$ 54.218,02

8. Levantamento de soluções

Haja vista que o firewall existente e o sistema atual de acessibilidade de dispositivo não suprem as necessidades e podem causar danos às atividades da Câmara é imprescindível encontrar soluções que atendam às demandas atuais. Desta forma, o levantamento de mercado possibilita encontrar a solução mais adequada. Sendo assim, dentre as soluções existentes no mercado, para o objeto do presente estudo foram encontradas as seguintes soluções:

Solução 01: Compra de firewall de próxima geração com fornecimento de equipamentos, software para o gerenciamento centralizado e emissão de relatórios detalhados, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução, licenciamento do software para atualizações e repasse tecnológico através de treinamento. Além da compra de equipamentos access point profissionais para promover a interconexão da rede cabeada com as diversas redes wireless. (Solução viável que permite sanar as necessidades).

Solução 02: Locação de firewall de próxima geração com fornecimento de equipamentos, software para o gerenciamento centralizado e emissão de relatórios detalhados, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução, licenciamento do software para atualizações e repasse tecnológico através de treinamento. Além da locação de equipamentos access point profissionais para promover a interconexão da rede cabeada com as diversas redes wireless. (Solução viável que permite sanar as necessidades).

9. Análise comparativa de soluções

Em análise as soluções viáveis 01 e 02 constatou-se os seguintes apontamentos:

Solução	Vantagens	Desvantagens
Solução 1 (Compra)	• A compra possibilita um controle personalizado e total sobre o sistema de firewall e access point, não havendo limitações sobre a disposição dos bens. • A compra permite a incorporação dos bens ao patrimônio da Câmara, não necessitando de pagamentos recorrentes. • A compra permite atualizações e manutenções imediatas por parte do Departamento de Tecnologia da Informação. • Não necessita de prorrogação contratual ou de novo contato para que a solução se mantenha.	• Alto custo inicial. • No caso de obsolescência a compra não permite a substituição dos equipamentos sem ser por meio de nova aquisição. • A compra dos equipamentos gera a necessidade de profissionais com conhecimento para gerir a tecnologia, necessitando assim de treinamento.
Solução 2 (Locação)	• A locação permite um baixo custo inicial. • A locação permite maior flexibilidade na troca dos equipamentos, devido às atualizações tecnológicas.	• A locação gera um menor controle e personalização uma vez que os equipamentos permanecem na propriedade do provedor.

		• A locação apesar do baixo custo inicial gera a necessidade de pagamentos recorrentes, que com o decorrer do tempo, quando somados podem superar o custo de compra dos equipamentos. • A locação gera dependência do locador, havendo risco do não cumprimento de todas as suas obrigações, fato este que pode gerar impactos até mesmo irreversíveis se tratando de segurança cibernética. • Necessita de prorrogação contratual ou de novo contato para que a solução se mantenha.

Desta forma se verifica que:

- Ambas possuem serviços de instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução, licenciamento do software para atualizações e repasse tecnológico através de treinamento.

- A compra dos equipamentos permite uma personalização detalhada para atender as especificidades do órgão, enquanto a locação gera dependência do provedor havendo risco do provedor não cumprir com a prestação do serviço esperado.
- A compra apesar de possuir um custo inicial elevado comparado com a locação, permite que os equipamentos integrem ao patrimônio da Casa Legislativa, ademais os pagamentos recorrentes da locação com o decorrer do tempo podem superar o custo de compra dos equipamentos.

Dado o exposto dentre as soluções viáveis a solução escolhida para suprir as necessidades foi a solução 01, por demonstrar-se mais vantajosa à administração, conforme verificado nos apontamentos acima descritos.

10. Registro de soluções consideradas inviáveis

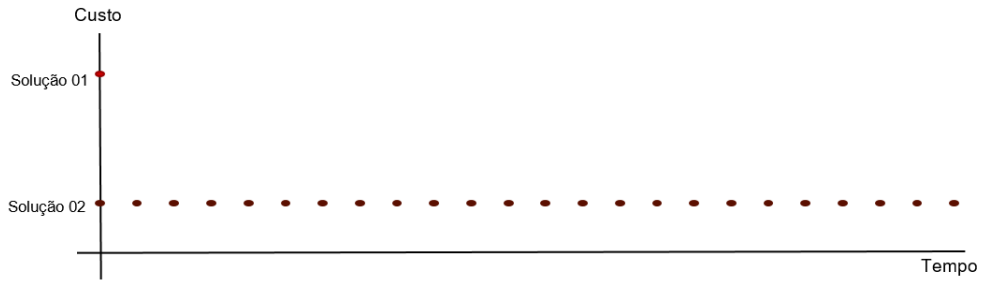
Não se aplica: não foram identificados impeditivos nas soluções levantadas que as possam classificar inviáveis.

11. Análise comparativa de custos (TCO)

Cabe ressaltar a importância de uma decisão ser fundamentada por uma análise ampla de diferentes fatores que possam influir sobre a pretendida resposta a ser dada à necessidade e suas consequências, portanto a decisão não foi amparada apenas pelo viés de custo, mas sim em seu custo benefício, ou seja, levou-se em consideração que o objeto a ser contratado não pode possuir eficiência, eficácia, e continuidade dúbia, além das características particulares do órgão. Os parâmetros decisórios levaram em consideração diferentes cenários que serão abordados a seguir.

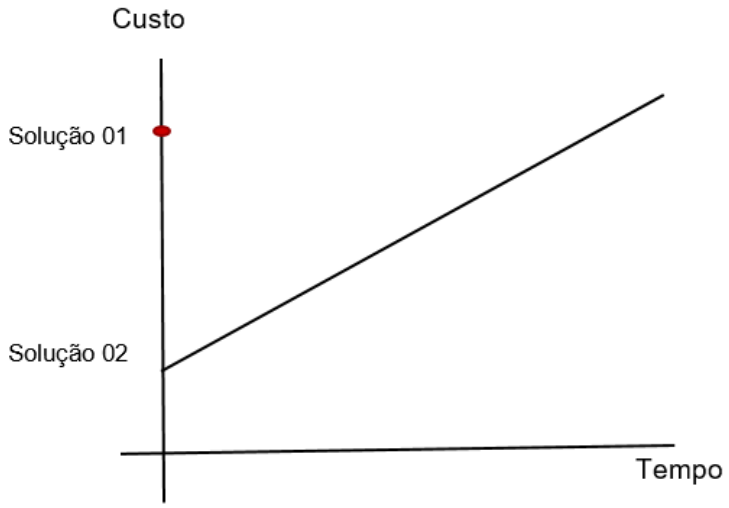
Ademais, em análise foi constatado a imprevisibilidade exata da duração da necessidade, uma vez que os dados e informações armazenados e utilizados por esta Casa Legislativa devem ser protegidos obrigatoriamente por lei, tal necessidade só deixaria de existir em virtude da revogação da lei ou pela vigência de nova lei que destituísse tal exigência. Portanto, considerando o objeto a ser contratado de necessidade contínua, pode se analisar o custo das soluções sobre a lógica matemática da seguinte maneira:

A solução 01 possui um custo imediato (inicial) alto o qual gera à administração a incorporação dos bens em seu patrimônio (representado por um único ponto no eixo vertical (Custo), uma vez que seu custo não se prolonga pelo eixo horizontal (Tempo)). Enquanto a solução 02 não permite a incorporação do bem ao patrimônio e possui um custo inicial inferior à solução 01, fato proveniente da característica do instituto da locação, em sua forma simples. Ademais, outro fato característico da locação é a continuidade de pagamentos para a sua manutenção, o que o torna um instituto recorrentemente praticado no mercado, haja vista que em certo ponto da variável Tempo ultrapassa-se o custo de compra. Portanto, trata-se de um instituto vantajoso para o locatário quando a sua necessidade não perdurar por um prolongado tempo que alcance o valor de custo.



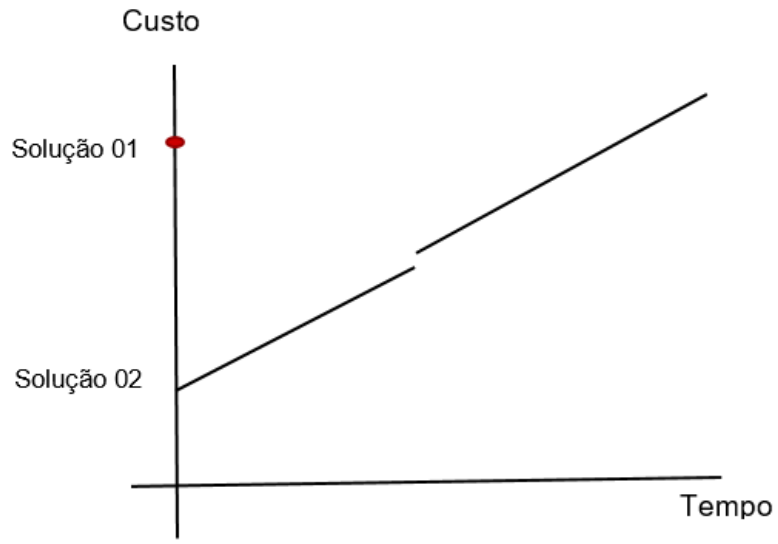
Este gráfico mostra ilustrativamente o investimento único da solução 01 e a continuidade de investimentos necessários para a manutenção da solução 02 (não se adotou nenhum número de parcelas, pois a necessidade do objeto a ser contratado é contínua não permitindo a fixação exata, pois findo uma variável Tempo pré-determinada haveria a necessidade de prolongamento da solução, seja por meio da prorrogação do contrato ou por um novo. Considerando a imprevisibilidade e de forma a não negligenciar a realidade fática descrita, considera a variável Tempo continua igualmente ao número de parcelas).

Cenário 1: cenário normal.



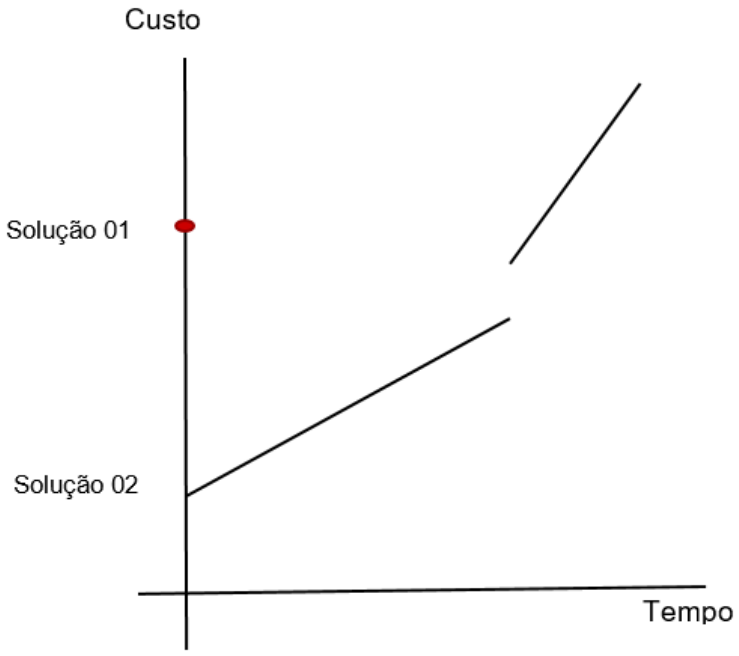
Este gráfico representa como no decorrer do tempo, somados os valores empregados na solução 02, o custo ultrapassa o da solução 01.

Cenário 2: cenário de infração.



Este gráfico mostra ilustrativamente o aumento por reajustes inflacionários, que decorrem de índices de correção inflacionárias previstos em contrato, os quais visam manter a vantajosidade a qual a contratada fazia jus ao início do contrato. É possível verificar que independentemente do valor do índice ele contribui para que o valor de custo da solução 01 seja alcançado mais rapidamente.

Cenário 3: cenário de caso fortuito ou força maior.



Este gráfico mostra ilustrativamente um cenário de aumento causado por motivos imprevisíveis que afetam todo o mercado, no qual resta à administração prover o restabelecimento econômico do contrato ou contratar com um custo mais elevado do que o anteriormente pretendido. É possível verificar que apesar de suas vantagens a solução 02 possui um risco no qual a administração não possui controle nem previsibilidade e pode sofre com a possibilidade de não conseguir contratar dada a imprevisibilidade de seu orçamento. Uma solução para tanto seria optar pela solução 01.

Portanto, a análise comparativa de custos levou em consideração diferentes cenários e identificou fatores que demonstram maior vantajosidade e controle de risco da contratação por meio da solução 01. Cabe ressaltar que a administração pública possui o dever de agir com responsabilidade dirimindo os riscos que porventura encontre, atendendo aos princípios da economicidade e eficiência.

12. Descrição da solução de TIC a ser contratada

A Câmara Municipal de Itabirito necessita dos serviços de atualização e adequação dos sistemas de segurança das redes de dados pois as versões gratuitas disponíveis não atendem as necessidades de controle e gerenciamento de rede e, ainda, não há atualmente equipamentos de hardware adequados para exercer as atividades de processamento de pacotes trafegados entre todos os dispositivos conectados e a internet. Desta forma, visa-se a contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall e access point, para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara Municipal de Itabirito.

Cabe ressaltar que a rede sem fio atual é disponibilizada por equipamentos que não são recomendados para ambientes institucionais o que gera impactos no desempenho das atribuições dos servidores por não possibilitar uma conexão com níveis de segurança desejáveis, nem alto desempenho, confiabilidade, gerenciamento e recursos avançados de autenticação.

Assim, a falta de proteção adequada da rede submete esta Casa Legislativa a diversos riscos de comprometimento de seus dados, tais como: dados corrompidos, deletados, sequestrados e vazados. Dada a gravidade dos prejuízos que a inércia de efetivação de uma solução eficaz para sanar as necessidades pode gerar, é de interesse público a contratação almejada.

A solução de firewall deve disponibilizar novos recursos customizados que permitam um melhor gerenciamento sobre as ameaças, facilidade na gestão e administração, interface intuitiva, suporte avançado personalizado e principalmente performance. Desta forma, faz-se necessária a adoção de um sistema moderno e robusto para manter os dados e informações da Câmara de Itabirito em segurança, protegendo contra invasões de hackers e evitando consequências que possam ser irreparáveis.

Para promover um gerenciamento centralizado de segurança apto a proteger a rede de ameaças externas e internas, bem como controlar o fluxo de dados entre essas redes e a Internet, a Câmara de Itabirito necessita de uma solução de firewall completa que permita:

- Gerenciamento avançado dos níveis de serviços;
- Visualização em tempo real das atividades exercidas na rede;
- Diminuição de intervenções humanas;
- Armazenamentos de históricos, gráficos e relatórios (por usuários e setores);
- Priorização de tráfegos por protocolos e aplicações;
- Balanceamento entre links de internet e controle de banda.

Portanto, a solução escolhida consiste na aquisição, na modalidade compra, de solução integrada em segurança e proteção da rede computacional com características de APPLIANCE DE NEXT GENERATION FIREWALL – NGFW (Firewall de próxima Geração), com fornecimento de equipamentos, software para o gerenciamento centralizado e emissão de relatórios detalhados, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução, licenciamento do software para atualizações e repasse tecnológico através de treinamento. Além de equipamentos de access points profissionais para promover a interconexão da rede cabeada com as diversas redes wireless.

Os fornecedores devem seguir as especificações dos itens descritos na tabela do item 7 do presente documento, conforme lhe tenha sido atribuído pelo processo licitatório. É necessário ressaltar que o processo licitatório se dará na modalidade de Pregão Eletrônico, considerando o disposto no artigo 6°, inciso XLI, da Lei 14.133/2021, no qual impõe a obrigatoriedade desta modalidade para a aquisição de serviços e bens comuns, sendo o critério de julgamento o de menor preço por lote.

Serão necessários para suprir a demanda e garantir a manutenção das atividades prestadas a aquisição de:

- Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) – Firewall de Próxima Geração com pacote de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de Firewall de Próxima Geração (NGFW): para proteção da rede. (1 unidade)
- Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) ou dispositivo remoto de ethernet – Firewall: para conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. (1 unidade)
- Equipamento Hardware Access Point – Ponto de Acesso Wireless: para transformação do sinal de rede a cabo em sinal de rede sem fio e de qualidade. (8 unidades)
- Serviços de instalação, configuração, implantação e migração de regras de Firewall e Access Point: para que seja possível a implementação das novas tecnologias. (1 unidade)
- Treinamento de configuração, gerência e operação do Firewall: para que seja possível suprir a demanda de forma eficaz. (1 unidade)
- Serviços de suporte e assistência técnica para operação e gerenciamento do Firewall e Access Point: para que seja possível suprir a demanda de forma eficaz. (12 meses)

13. Estimativa de custo total da contratação

Valor (R$): 195.487,27

O custo unitário estimado da contratação por item é de:

- R$ 39.680,88 para Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) – Firewall de Próxima Geração – Equipamento com suporte a cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo. Com 03 anos de suporte e garantia de hardware. Pacote de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de Firewall de Próxima Geração (NGFW) pelo prazo de 36 (trinta e seis) meses;
- R$ 15.461,00 para Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) ou dispositivo remoto de ethernet – Firewall ou dispositivo deve oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. Deve funcionar em conjunto com o equipamento de firewall (item 01).
- R$ 7.720,82 para HARDWARE ACCESS POINT – Ponto de Acesso Wireless com Rádio Duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples, incluindo adaptador PoE.
- R$ 18.160,83 para Serviços de instalação, configuração, implantação e migração de regras de Firewall e Access Point.
- R$ 6.200,00 para Treinamento de configuração, gerência e operação do Firewall. A transferência de conhecimento deve ter um total mínimo de 20 horas, feito por profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.
- R$ 4.518,17 para Serviços de suporte e assistência técnica para operação e gerenciamento do Firewall e Access Point.

O custo total estimado da contratação por item é de:

- R$ 39.680,88 para Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) – Firewall de Próxima Geração – Equipamento com suporte a cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo. Com 03 anos de suporte e garantia de hardware. Pacote de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de Firewall de Próxima Geração (NGFW) pelo prazo de 36 (trinta e seis) meses;
- R$ 15.461,00 para Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) ou dispositivo remoto de ethernet – Firewall ou dispositivo deve oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. Deve funcionar em conjunto com o equipamento de firewall (item 01).
- R$ 61.766,53 para HARDWARE ACCESS POINT – Ponto de Acesso Wireless com Rádio Duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples, incluindo adaptador PoE.
- R$ 18.160,83 para Serviços de instalação, configuração, implantação e migração de regras de Firewall e Access Point.
- R$ 6.200,00 para Treinamento de configuração, gerência e operação do Firewall. A transferência de conhecimento deve ter um total mínimo de 20 horas, feito por profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.
- R$ 54.218,02 para Serviços de suporte e assistência técnica para operação e gerenciamento do Firewall e Access Point.

Justificativa do preço: a estimativa de preços se deu mediante comprovação dos preços praticados por outras administrações mediante consulta em sites e por consultas a fornecedores, conforme mapa de preços em anexo.

14. Justificativa técnica da escolha da solução

A escolha de uma solução de Firewall de Próxima Geração (NGFW) se justifica por conceder análises não apenas do tráfego nas camadas 3 e 4, como um firewall tradicional, mas atuar até a camada 7. Essa característica é fator decisivo para se optar por esse recurso tecnológico, uma vez que permite:

- Uma segurança mais robusta a ameaças sofisticadas;
- Maior controle sobre o tráfego de sua rede, com maior visibilidade e detalhamento das atividades;
- Um gerenciamento de segurança de rede simplificado, por possuir uma interface centralizada para o gerenciamento de políticas de segurança;
- A otimização da configuração, monitoramento e atualização das regras;
- Alto desempenho.

A escolha se uma solução de Ponto de Acesso Wireless ao invés dos access points tradicionais, se motiva pelos seguintes aspectos:

- Supre demandas mais robustas, com grande densidade de conexões;
- Permite recursos avançados de autenticação;
- Alto desempenho;
- Alta abrangência do sinal;
- Estabilidade do sinal;
- Proporciona maior segurança a rede.

Já a solução de serviço de instalação, de configuração, de assistência técnica e treinamento se justifica por se tratar de uma tecnologia ainda não utilizada pelo órgão, a qual a sua equipe do Departamento de Tecnologia da Informação ainda não possui contato. Portanto, é imprescindível para a viabilidade da solução como um todo a contratação desses serviços.

15. Justificativa econômica da escolha da solução

Baseando-se na comparação de custos realizada no item 11 deste documento, a contratação da solução 01 (Compra de firewall de próxima geração com fornecimento de equipamentos, software para o gerenciamento centralizado e emissão de relatórios detalhados, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução, licenciamento do software para atualizações e repasse tecnológico através de treinamento. Além da compra de equipamentos access points profissionais para promover a interconexão da rede cabeada com as diversas redes wireless) demonstrou ser mais econômica em comparação a outra solução por não ultrapassar o custo de compra.

Para mais, em termos de economicidade será adotada a divisão em lote. Sendo assim, a licitação será dividida em 2 lotes distintos, os quais separam equipamentos de serviços e visa a compatibilidade dos equipamentos e serviços, para que não haja prejuízo para o conjunto e a necessidade de novos gastos, sendo subdividida em 6 (seis) itens. A contratação se dará por menor preço por lote.

Esta decisão se justifica por existir inúmeras marcas de equipamentos para compor um sistema Firewall e incontáveis modelos de Access Points no mercado, devido a essa diversidade há também vários tipos de configurações e métodos de instalação para que o sistema Firewall funcione em sincronia com os dispositivos de acesso sem fio.

O agrupamento dos itens evita que haja conflitos e incompatibilidade dos recursos tecnológicos, pois cada fornecedor trabalha com equipamentos específicos e possuem diferentes metodologias de instalação. Não se demonstra viável para a administração licitar somente parte dos itens, pois todos os componentes deverão ser instalados em conjunto para que o sistema de segurança e de acesso funcionem de maneira correta. Além disso, os itens agrupados possuem similaridade e guardam relação entre si, não comprometendo a competitividade do certame.

Portanto, a opção pela indivisibilidade do objeto é uma ação cautelosa definida pelo Departamento de Tecnologia da Informação desta casa legislativa que avaliou as peculiaridades envolvidas e identificou possíveis problemas na implantação do sistema. Todas análises foram feitas para assegurar a compatibilidade entre os itens e ainda assim manter a competitividade necessária à disputa, garantindo com que o licitante atue de forma independente.

16. Benefícios a serem alcançados com a contratação

A aquisição do Access Point beneficia os servidores e colaboradores permitindo que estes utilizem para o auxílio de suas atribuições dispositivos sem a necessidade da conexão por cabo, abrangendo assim a utilização de um maior quantitativo de dispositivos. Assim consequentemente contribui com a melhoria na prestação dos serviços ofertados pela Câmara Municipal de Itabirito. Ademais, a utilização de equipamentos adequados para a disponibilização da rede sem fio permite maior segurança e controle da rede, amenizando os riscos de ataques cibernéticos e futuros prejuízos.

Assim também, a contratação de uma solução de Firewall adequada às necessidades desta Casa Legislativa gera benefícios, oferecendo proteção adequada da rede, defesa proativa e operações simplificadas de controle do tráfego da rede, criando uma rede segura, protegendo dados, ajudando a prevenir ataques de hackers, malwares, tentativas de invasão e contribuindo para a não paralisação das atividades causadas por possíveis danos à rede. Além de permitir adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

Desta forma, a aquisição dos itens dispostos na tabela do item 7, implicará no atendimento das necessidades supracitadas no item 2. De modo a beneficiar os servidores e usuários da Câmara Municipal de Itabirito, concedendo-lhes a manutenção e proteção das atividades desta Casa Legislativa. Ou seja, a contratação resultará em melhoria na qualidade e segurança da prestação de serviços.

Para além, o procedimento almejado propicia à administração conformidade com as normativas legais vigentes, os princípios da legalidade, finalidade, motivação, razoabilidade, proporcionalidade, interesse público, eficiência. Assim sendo, a almejada contratação atende aos princípios regentes da licitação pública e supre as necessidades dispostas neste estudo.

17. Providências a serem Adotadas

Com o exposto, conclui-se que deve ser formalizado pregão eletrônico, nos termos do art. 6°, XLI, da Lei nº 14.133 /2021, seguindo com a elaboração do termo de referência e demais atos posteriores até a elaboração do respectivo instrumento contratual.

Além das ações acima, o setor competente deverá:

- Verificar a regularidade jurídica, fiscal, trabalhista e técnica da pessoa física ou jurídica;

- Verificar a disponibilidade financeira e orçamentária para cobrir a despesa.

18. Contratações Correlatas ou Interdependes

Não há serviços correlatos nem interdependentes com esta contratação.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

Após concluir os Estudos Técnicos Preliminares aqui registrados, em relação à viabilidade da contratação, constata:

A relação custo-benefício da contratação é considerada favorável.

Os requisitos relevantes para contratação foram adequadamente levantados e analisados.

Assim, considerando os pontos listados acima, entendemos ser VIÁVEL e NECESSÁRIA a contratação da solução demandada.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

LAYANE CRISTINE FARIA ANDREWS

Chefe de Departamento Administrativo

Assinou eletronicamente em 15/01/2025 às 14:57:24.

FILIPE AUGUSTO SERRA PALHEIROS

Chefe de TI

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - MAPA DE PREÇOS.pdf (596.38 KB)
- Anexo II - Análise de risco - Firewall.pdf (572.51 KB)

ITEM	QUANTIDADE	OBJETO - Contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall e access point, para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara de Itabirito	Clínica Do Micro	Segmento Digital Com. Ltda
1	1	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) – Firewall de Próxima Geração – Equipamento com suporte a cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo. Com 03 anos de suporte e garantia de hardware. Pacote de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para *appliance de Firewall de Próxima Geração (NGFW)* pelo prazo de 36 (trinta e seis) meses.	R$ 39.647,28	R$ 37.198,00
2	1	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) ou dispositivo remoto de ethernet – Firewall ou dispositivo deve oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. Deve funcionar em conjunto com o equipamento de firewall (item 01).	R$ 16.125,20	R$ 15.452,00
3	8	HARDWARE ACCESS POINT – Ponto de Acesso Wireless com Rádio Duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples, incluindo adaptador PoE.	R$ 7.095,25	R$ 7.082,15
4	1	Serviços de instalação, configuração, implantação e migração de regras de Firewall e Access Point.	R$ 15.000,00	R$ 15.200,00
5	1	Treinamento de configuração, gerência e operação do Firewall. A transferência de conhecimento deve ter um total mínimo de 20 horas, feito por profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.	R$ 6.000,00	R$ 6.000,00
6	12	Serviços de suporte e assistência técnica para operação e gerenciamento do Firewall e Access Point.	R$ 4.590,00	R$ 4.550,00

Identificação do servidor responsável pela cotação: Valdir José de Morais - CPF: 724.144.646 - 15 **DATA 19.09**

Fontes consultadas: Para elaboração da pesquisa de preços foi utilizados os seguintes parâmetros, empregados de forma combinada:

Cotação Zenite. Valor adjudicados em Licitação de orgão público constante da cotação: INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NA
compra?compra=15812405000532023; Conselho Regional de Educação Física da 2ª Região - CREF2/RS https://cnetmobile.estaleiro.serpro.gov.br/compr
Administração SPOA/SE/Minc https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=420001
MUNICIPAL DE MARINGA - PR https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=987691
compra?compra=08002505000192023; SERVIÇO SOCIAL DO COMERCIO SESC ADMINISTRAÇÃO REGIONAL NO ESTADO DO TOCANTINS https://cnetmob
DO ESTADO DE SÃO PAULO ESP-EMPRESA METROPOLITANA DE TRANSPORTES URBANOS DE SAO PAULO SA https://cnetmobile.estaleiro.serpro.gov.br/
Pesquisa direta com cinco fornecedores, três responderam. Método matemático aplicado para definição do valor estimado. Valor médio.

Para realização da pesquisa de preço foram observadas condições comerciais praticadas, incluindo prazos e locais de entrega, formas de pagamento e fr

Conforme o Decreto Municipal nº 14.754/2023:
* Foram desconsiderados os valores excessivos, calculados conforme o Art. 47, §3º I: aqueles que sejam superiores a 30% (trinta por cento) da média do
** Foram desconsiderados os valores inexequíveis, calculados conforme o Art. 47, §3º II: aqueles que sejam inferiores a 70% (setenta por cento) da méd

Para realização da pesquisa de preço foram observadas condições comerciais praticadas, incluindo prazos e locais de entrega, formas de pagamento e fr
O objetivo da pesquisa foi determinar o preço estimado para a aquisição dos bens, conforme os padrões estabelecidos no art. 46º, incisos IV e II, do Decr
I - Realização de pesquisa direta com, no mínimo, três fornecedores, por meio de solicitação formal de cotação via ofício ou e-mail;
II - Consideração de contratações similares realizadas pela Administração Pública, no período de até um ano anterior à data da pesquisa, incluindo aquel

Para a escolha dos fornecedores cotados, adotamos os seguintes métodos:
Pesquisa direta via e-mail: A seleção dos fornecedores foi feita com base na análise de relatórios de licitações eletrônicas anteriores para aquisição de be
Análise de contratações similares pela Administração Pública: Foram realizadas pesquisas em sites governamentais, como o Comprasnet e o Portal Nacio

Nos autos da contratação correspondente da relação de 12 (doze) fornecedores que foram consultados, 03 (três) enviaram resposta.

Braga & Fontes Informática Ltda (Prolinx)	INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NATURAIS RENOVÁVEIS	INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO	Conselho Regional de Educação Física da 2ª Região - CREF2/RS	Assembleia Legislativa do Estado de Rondônia – ALE/RO	Ministério da Cultura - Subsecretaria de Planejamento, Orçamento e Administração SPOA/SE/Minc	PREFEITURA MUNICIPAL DE SANTA LUZIA/MG
R$ 33.270,85	R$ 41.050,00	R$ 43.200,00				
R$ 10.347,82		R$ 19.780,00	R$ 15.600,00			
R$ 6.877,50				R$ 8.800,00	R$ 7.600,00	R$ 8.870,00
R$ 14.000,00						
R$ 4.000,00						
R$ 3.000,00						

.2024

ATURAIS RENOVÁVEIS https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=193099059001520
rasnet-web/public/compras/acompanhamento-compra?compra=92733805900062024; Assembleia Legislativa do Estado de Rondônia – ALE/RO https://cnet
05000092023; PREFEITURA MUNICIPAL DE SANTA LUZIA/MG http://comprasnet.gov.br/livre/pregao/termoHom.asp?prgCod=1158215&tipo=t; CONSELHO
.05900812024; Instituto Federal de Educação, Ciencia e Tecnologia de Roraima - Campus Zona Oeste https://www.comprasnet.gov.br/acesso.asp?url=/edita
ile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=92812005900132024; MINISTÉRIO DA GESTÃO E DA INOV
'comprasnet-web/public/compras/acompanhamento-compra?compra=37340105900062024.

etes.

s demais preços.
ia dos demais preços.

etes.
reto Municipal nº 14.754/2023, utilizando os seguintes critérios:

as feitas por meio de sistema de registro de preços, com a devida atualização dos valores.

ens similares em cidades da região (Grande BH e região dos Inconfidentes), obtendo informações relevantes sobre fornecedores para esta cotação.
onal de Contratações Públicas (PNCP), para identificar e analisar contratações similares e obter referências adicionais sobre fornecedores e valores praticado

CONSELHO REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO	PREFEITURA MUNICIPAL DE MARINGA - PR	Instituto Federal de Educação, Ciencia e Tecnologia de Roraima - *Campus* Zona Oeste	TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT)	SERVIÇO SOCIAL DO COMERCIO SESC ADMINISTRAÇÃO REGIONAL NO ESTADO DO TOCANTINS	MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS ARQUIVO NACIONAL	GOVERNO DO ESTADO DE SÃO PAULO ESP-EMPRESA METROPOLITANA DE TRANSPORTES URBANOS DE SAO PAULO SA.
		R$ 42.000,00		R$ 41.400,00		
R$ 24.615,00	R$ 23.150,00	R$ 31.000,00 **			R$ 17.000,00	
		R$ 19.000,00 **	R$ 7.500,00	R$ 7.500,00		
	R$ 4.000,00			R$ 9.900,00 **	R$ 4.469,01	R$ 6.500,00

24; INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acom
:mobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?compra=92691905900062024; Ministério da Cultura - Subsecr
REGIONAL DE QUÍMICA IV REGIÃO – SÃO PAULO https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra?c
l-158352-5-11-2023; TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO (MT) https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras
AÇÃO EM SERVIÇOS PÚBLICOS - ARQUIVO NACIONAL https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-comp

s.

VALOR MÉDIO	VALOR GLOBAL
R$ 39.680,88	R$ 39.680,88
R$ 15.461,00	R$ 15.461,00
R$ 7.720,82	R$ 61.766,53
R$ 18.160,83	R$ 18.160,83
R$ 6.200,00	R$ 6.200,00
R$ 4.518,17	R$ 54.218,02
TOTAL	**R$ 195.487,27**

ıpanhamento-
etaria de Planejamento, Orçamento e
ompra=92518105900102024; PREFEITURA
;/acompanhamento-
ra?compra=20024705900062024; GOVERNO

ANEXO
ANÁLISE DE RISCOS

INTRODUÇÃO
Tendo em vista que a Análise de Riscos irá descrever e avaliar as ameaças que possam vir a comprometer o sucesso e objetivo da contratação, bem como definir de que formas devem ser tratadas, **ela permeará todo processo de contratação**

1 – RISCOS DA FASE DO PLANEJAMENTO DA CONTRATAÇÃO E SELEÇÃO DO FORNECEDOR		
Risco 01:	**Seleção infrutífera devido ao baixo preço de referência**	
Probabilidade:	Baixa	
Id	**Dano**	**Impacto**
1.	Caso a seleção reste infrutífera, devido ao baixo preço de referência, causará impacto considerável para os resultados como um todo, sobretudo para as próximas etapas de contratação.	Alto
Id	**Ação Preventiva**	**Responsável**
1.	Realização de pesquisa a fornecedores e utilização de preço mediano, desprezando-se a influência de valores extremamente altos ou baixos.	Setor de licitação, compras e contratos
Id	**Ação de Contingência**	**Responsável**
1.	Revisão dos preços e republicação do Aviso.	Setor de licitação, compras e contratos

Risco 02:	**Incompatibilidade com sistemas existentes**

Probabilidade:	Média	
Id	**Dano**	**Impacto**
1.	Interrupção ou falha na integração com a infraestrutura de rede atual.	Médio
Id	**Ação Preventiva**	**Responsável**
1.	Realizar levantamento técnico detalhado.	Setor requisitante.
Id	**Ação de Contingência**	**Responsável**
1.	Reavaliar a arquitetura da rede.	Setor requisitante.

Risco 03:	**Subdimensionamento do equipamento**	
Probabilidade:	Média	
Id	**Dano**	**Impacto**
1.	Degradação do desempenho da rede devido à alta demanda.	Alto
Id	**Ação Preventiva**	**Responsável**
1.	Análise de capacidade detalhada e planejamento para crescimento futuro.	Setor requisitante.
Id	**Ação de Contingência**	**Responsável**
1.	Contratar um equipamento adicional ou redistribuir a carga na rede.	Setor de licitação, compras e contratos / Setor requisitante.

Risco 04:	**Licenciamento incompatível**	
Probabilidade:	Média	
Id	**Dano**	**Impacto**
1.	Funcionalidades limitadas ou custo elevado inesperado.	Médio
Id	**Ação Preventiva**	**Responsável**
1.	Revisar detalhadamente o modelo de licenciamento e prever expansões.	Setor requisitante.
Id	**Ação de Contingência**	**Responsável**
1.	Negociar ajuste contratual ou adquirir licenças adicionais.	Setor de licitação, compras e contratos

2 – RISCOS DA FASE DE EXECUÇÃO		
Risco 05:	**Configuração incorreta**	
Probabilidade:	Média	
Id	**Dano**	**Impacto**
1.	Vulnerabilidades de segurança e falhas no desempenho do firewall.	Alto
Id	**Ação Preventiva**	**Responsável**
1.	Garantir suporte especializado na configuração e auditorias técnicas.	Setor requisitante.
Id	**Ação de Contingência**	**Responsável**
1.	Realizar reconfiguração imediata com suporte técnico avançado.	Órgão demandante.

Risco 06:	**Tempo de instalação acima do previsto**	
Probabilidade:	Média	
Id	**Dano**	**Impacto**
1.	Atraso no cronograma e impacto no funcionamento da rede.	Alto
Id	**Ação Preventiva**	**Responsável**
1.	Planejamento detalhado e contratação de equipe experiente.	Setor de licitação, compras e contratos
Id	**Ação de Contingência**	**Responsável**
1.	Ajustar cronogramas e priorizar etapas críticas.	Setor requisitante.

ANEXO III

MODELO DE PROPOSTA DE PREÇOS

OBJETO: Contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall e access point, para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara de Itabirito

DATA DE APRESENTAÇÃO DA PROPOSTA: _____

LOTE 1 – Firewall e Access Point							
ITEM	**ESPECIFICAÇÃO**	**CATMAT**	**UNIDADE DE MEDIDA**	**QUANTIDADE**	**MARCA**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) – Firewall de Próxima Geração – Equipamento com suporte a cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo. Com 03 anos de suporte e garantia de hardware. Pacote de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para *appliance de Firewall de Próxima Geração (NGFW)* pelo prazo de 36 (trinta e seis) meses.	609340	Unidade	1			

2	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) ou dispositivo remoto de ethernet – Firewall ou dispositivo deve oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. Deve funcionar em conjunto com o equipamento de firewall (item 01).	609340	Unidade	1			
3	HARDWARE ACCESS POINT – Ponto de Acesso Wireless com Rádio Duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples, incluindo adaptador PoE.	605537	Unidade	8			

LOTE 2 – Serviço de instalação, configuração e treinamento						
ITEM	**ESPECIFICAÇÃO**	**CATSER**	**UNIDADE DE MEDIDA**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
4	Serviços de instalação, configuração, implantação e migração de regras de Firewall e Access Point.	26972	Unidade	1		
5	Treinamento de configuração, gerência e operação do Firewall. A transferência de conhecimento deve ter um total mínimo de 20 horas, feito por profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento,	3840	Unidade	1		

	Centralização e Monitoração de Logs Centralizado.					
6	Serviços de suporte e assistência técnica para operação e gerenciamento do Firewall e Access Point.	26999	Mês	12		

- Dados Bancários para pagamento:
- Prazo de validade da proposta não inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

Local, (data).

(Assinatura do representante legal)

ANEXO IV

MINUTA DO CONTRATO

CONTRATO Nº _____/2024

PROCESSO ADMINISTRATIVO N° 465/2024

PREGÃO N° 10/2024

Por este instrumento particular de contrato, de um lado, a **CÂMARA MUNICIPAL DE ITABIRITO**, CNPJ 18.366.963/0001-79, Inscrição Estadual: Isento, com sede administrativa à Avenida Queiroz Júnior, nº 639, Bairro Praia, Itabirito/MG, CEP: 35.450-228, fone/fax: (31) 3561-1599, representada pelo Presidente, Vereador ANDERSON MARTINS DA CONCEIÇÃO, portador do CPF nº 058.156.676-92 e da Carteira de Identidade nº MG-11.253.680 - SSP/MG, expedida pela SSP/MG, residente e domiciliado em Itabirito/MG, de agora em diante denominada CONTRATANTE e de outro lado, _____, inscrita no CNPJ _____, com endereço na rua/av. _____, nº _____, bairro _____, cidade/estado, CEP: _____, neste ato representada por seu sócio _____, brasileiro(a), estado civil, profissão, portador(a) do CPF nº _____ e da identidade nº _____, residente em _____, de agora em diante denominada CONTRATADA, celebram o presente contrato de acordo com a Lei nº 14.133/2021 e de acordo com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - Do Procedimento para Contratação

1.1- Este contrato foi autorizado pelo Processo Administrativo nº 465/2024, Pregão Eletrônico nº **10/2024**, em conformidade com o art. 6º, alínea XLI, da Lei nº 14.133/2021.

CLÁUSULA SEGUNDA - Do Objeto

2.1- Este contrato tem como objeto: Contratação de empresa especializada para fornecimento, instalação e configuração de solução de firewall e access point, para ampliação da acessibilidade, segurança, proteção de rede, gerenciamento e modernização do Data Center da Câmara de Itabirito

LOTE 1 – Firewall e Access Point						
ITEM	**ESPECIFICAÇÃO**	**CATMAT**	**UNIDADE DE MEDIDA**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) –	609340	Unidade	1		

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

	Firewall de Próxima Geração – Equipamento com suporte a cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo. Com 03 anos de suporte e garantia de hardware. Pacote de licenças de firewall, IPS, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para *appliance de Firewall de Próxima Geração (NGFW)* pelo prazo de 36 (trinta e seis) meses.					
2	Equipamento Hardware de proteção de Rede NGFW (Next-Generation Firewall) ou dispositivo remoto de ethernet – Firewall ou dispositivo deve oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos. Deve funcionar em conjunto com o equipamento de firewall (item 01).	609340	Unidade	1		
3	HARDWARE ACCESS POINT – Ponto de Acesso Wireless com Rádio Duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples, incluindo adaptador PoE.	605537	Unidade	8		

LOTE 2 – Serviço de instalação, configuração e treinamento						
ITEM	**ESPECIFICAÇÃO**	**CATSER**	**UNIDADE DE MEDIDA**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

4	Serviços de instalação, configuração, implantação e migração de regras de Firewall e Access Point.	26972	Unidade	1		
5	Treinamento de configuração, gerência e operação do Firewall. A transferência de conhecimento deve ter um total mínimo de 20 horas, feito por profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.	3840	Unidade	1		
6	Serviços de suporte e assistência técnica para operação e gerenciamento do Firewall e Access Point.	26999	Mês	12		

2.2- Vinculam esta contratação, independentemente de transcrição:
- Termo de Referência;
- Edital de licitação;
- Proposta do contratado;
- eventuais anexos dos documentos supracitados.

CLÁUSULA TERCEIRA - Modelo de Gestão do Contrato

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

3.2- Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

3.3- A Câmara Municipal fiscalizará a execução do objeto deste contrato, na forma da lei nº 14.133/2021, do Decreto Municipal nº 14.754/2023 e da Resolução nº 01/2024 desta Câmara.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

3.4- O(a) fiscal do contrato será o(a) servidor(a) Jussara Maria Pereira e o(a) gestor(a) do contrato será o(a) servidor(a) Layane Cristine Faria Andrews.

3.5- Após a assinatura do contrato ou instrumento equivalente, a Câmara terá a faculdade de convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados, dentre outros.

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

3.7- A fiscalização do objeto do contrato pela Contratante não exclui a responsabilidade da Contratada por qualquer inobservância ou omissão à legislação vigente e às cláusulas contratuais do Contrato.

3.8- O Contratado é obrigado a assegurar e facilitar o acompanhamento da execução do contrato pela Contratante, bem como permitir o acesso a informações consideradas necessárias.

3.9- As atividades de gestão e de fiscalização do contrato deverão ser realizadas de forma preventiva, rotineira e sistemática e exercidas por agentes públicos ou por equipe de fiscalização.

CLÁUSULA QUARTA - Das Obrigações das Partes

4.1- Da Contratada:

Regime de execução ou forma de fornecimento

O fornecimento/a prestação do serviço será: continuado.

Início da execução do objeto: após emissão da ordem de serviço.

Prazo de entrega do bem ou execução do serviço: os serviços deverão ser realizados no prazo máximo de 15 (quinze) dias úteis após a data da entrega dos equipamentos

Local de entrega ou de execução do serviço: Sede da Câmara de Itabirito localizada na Av. Queiroz Junior nº 639, Bairro Praia, Itabirito MG. Centro de atendimento ao Cidadão e Gabinete dos Vereadores localizados na rua José Benedito n°189 - 3° andar, bairro Santa Efigênia, Itabirito MG

MODELO DE EXECUÇÃO DO OBJETO

DESCRIÇÃO DE SOLUÇÃO DE SEGURANÇA DE REDE – NGFW (ITEM 1)

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares*, Filtro de URL, criptografia de e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.

Dispositivo remoto de ethernet, para oferecer conectividade de borda para locais remotos, que deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso seguro aos recursos remotos.

Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / *malwares,* assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período mínimo de 36 (trinta e seis) meses.

Para os itens que representem bens materiais, a **CONTRATADA** deverá fornecer produtos novos, sem uso anterior.

Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento.

Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).

Por alta disponibilidade (HA) entende-se que a solução deverá ser composta ao menos por dois *appliances*, licenciados para funcionamento em redundância.

A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um equipamento (sempre em modo de alta disponibilidade HA) para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Cada *appliance* deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

DESCRIÇÃO E CARACTERÍSTICAS DE FIREWALL (NGFW) OU DISPOSITIVO REMOTO DE ETHERNET (ITEM 2)

Deve ser do mesmo fabricante do firewall e em forma de appliance.

Deve ter a funcionalidade de conectar a matriz e direcionar todo o tráfego via túnel seguro de forma a fornecer acesso aos recursos remotos.

O túnel seguro deve ter no mínimo 850 Mbps de throughput utilizando criptografia AES256 e TLS 1.2.

Deve suportar módulo adicional de Wi-fi MIMO 2x2:2, com rádio padrão mínimo 802.11 a/b/g/n/ac Wave 1 (Wi-Fi 5), habilitado para banda dupla ou 4G/LTE.

Deve possuir no mínimo 04(quatro) interfaces 10/100/1000 Base-TX (1 GbE de cobre).

Deve possuir no mínimo 02(duas) interfaces USB 3.0. Possuir luzes indicativas no mínimo equipamento ligado, interface de rede ligada.

Possuir fonte de alimentação bivolt compatível com 110-240 V, 50-60 Hz. (RED15/REDE15w).

Deve suportar 2a fonte de alimentação.

Possuir no mínimo as certificações CE/FCC/IC/RCM/VCCI/CB/UL/CCC/KC/ANATEL.

Operar com humidade de no mínimo entre 10% a 90%, sem condensação.

Deve ser possível ser gerenciado pelo equipamento concentrador.

Deve ser possível pelo equipamento concentrador atualizar todos os firmwares de forma a facilitar a manutenção.

Deve ser permitir carregar a configuração por USB ou de forma automática.

Uplink deve permitir a configuração estática de IP ou através de DHCP.

Deve possuir a funcionalidade de gerenciar o DHCP de forma centralizada.

Deve possuir alta disponibilidade implementando fail-over nos túneis com a matriz.

Deve possuir a funcionalidade de balanceamento entre dois túneis com a matriz.

Para facilitar a implementação de regras específicas por regiões deve aparecer como interface no concentrador central.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Para facilitar a implementação de regras específicas deve possuir funcionalidade de agregar logicamente todas as localidades como uma interface no concentrador central.

Deve ter a funcionalidade de compressão do túnel de forma a otimizar a banda utilizada.

Deve possuir a funcionalidade de filtrar por MAC.

CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DO FIREWALL DE PRÓXIMA GERAÇÃO - NGFW

Performance mínima de 10.500 Mbps de *throughput* para firewall.

Performance mínima de 2.500 Mbps de throughput para firewall NGFW.

Performance mínima de 3.250 Mbps de throughput de IPS.

Performance mínima de 900 Mbps de throughput para controle de AV/proxy.

Performance mínima de 1.800 Mbps de throughput de VPN.

Suporte a, no mínimo, 5.000.000 (5 milhões) de conexões simultâneas.

Suporte a, no mínimo, 69.900 (sessenta e nove mil e novecentos) novas conexões por segundo.

Possuir o número irrestrito quanto ao máximo de usuários licenciados.

Possuir armazenamento interno de no mínimo 64 GB SSD para sistema operacional, quarentena local, logs e relatórios.

Possuir no mínimo 4GB de memória RAM.

Possuir no mínimo 12 (doze) interfaces de rede GbE1000Base-TX.

Possuir no mínimo 2 (duas) interfaces SFP Fiber.

Possuir no mínimo 1 (um) módulo de expansão de interfaces.

Possuir 1 (uma) interface do tipo console ou similar.

CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO

O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), console de gerência, monitoração e logs.

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários, controle granular de permissões, IPS, Firewall, Antispam, VPN IPSec, SSL VPN e SSL Inspection.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação técnica.

Todos os equipamentos fornecidos poderão ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

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

O software deverá ser fornecido em sua versão mais atualizada.

A solução deverá ter capacidade de operar em alta Disponibilidade (HA). O HA deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.

Uma interface completa de comando de linha (*CLI command-line-interface*) deverá ser acessível através da interface gráfica e via porta serial.

A atualização de software deverá enviar avisos de atualização automáticos.

O sistema de objetos deverá permitir a definição de redes, serviços, *hosts* períodos de tempos, usuários e grupos, clientes e servidores.

O *backup* e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

As notificações deverão ser realizadas via e-mail e SNMP.

Suportar SNMPv3 e Netflow.

O firewall deverá ser *stateful*, com inspeção profunda de pacotes.

As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

As políticas de NAT deverão ser customizáveis para cada regra.

A proteção contra *flood* deverá ter proteção contra DoS (*Denial of Service*), DdoS (*Distributed DoS*).

Proteção contra *anti-spoofing*.

Suportar IPv4 e IPv6.

IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e *IPv6 Rapid Deployment (6rd)* de acordo com a RFC 5969.

Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Deve possuir tecnologia de conectividade SD-WAN;

A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN;

Deve implementar balanceamento entre os links WAN com método SpillOver;

Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN;

Deve suportar o uso de, no mínimo, 3 (três) links;

Deve suportar o uso de links de interfaces físicas, subinterfaces lógicas de VLAN e túneis IPSec;

Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde;

A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima;

Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês;

A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoE configurado;

A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador;

Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;

A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados;

Deve possibilitar o roteamento baseado em VPNs;

Deve suportar criar políticas de roteamento;

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:

Interface de entrada do pacote;

IPs de origem;

IPs de destino;

Portas de destino;

Usuários ou grupos de usuários;

Aplicação em camada 7.

Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento;

Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e *tagging* de VLAN.

Deve suportar Extended VLAN;

O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, *failover* automático e balanceamento por peso.

A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

Deve permitir a configuração de jumbo frames nas interfaces de rede;

Deve permitir a criação de um grupo de portas layer2;

A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal;

A solução deverá permitir configurar os serviços de DNS, *Dynamic* DNS, DHCP e NTP;

O *traffic shapping (QoS)* deverá ser baseado em rede ou usuário.

A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

Deve possuir otimização em tempo real de voz sobre IP.

Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

CONTROLE POR POLÍTICAS DE FIREWALL

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

Controle de políticas por países via localização por IP.

Suporte a objetos e regras IPV6.

Suporte a objetos e regras *multicast*.

PREVENÇÃO DE AMEAÇAS

Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, *Anti-Malware* e Firewall de Proteção Web (*WAF*) integrados no próprio *appliance* de Firewall ou entregue em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

Deve suportar granularidade nas políticas de IPS Antivírus e *Anti-Malware*, possibilitando a criação de diferentes politicas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;

A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em núvem;

Para a eficácia da análise de malwares Zero-Days, a solução de Sandobox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning;

A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma;

Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em núvem;

A proteção *Anti-Malware* deverá bloquear todas as formas de vírus, *web malwares*, *trojans* e *spyware* em HTTP e HTTPS, FTP e *web-e-mails*.

A proteção Anti-Malware deverá realizar a proteção com emulação *JavaScript*.

Deve ter proteção em tempo real contra novas ameaças criadas.

Deve possuir pelo menos duas *engines* de anti-vírus independentes e de diferentes fabricantes para a detecção de *malware*, podendo ser configuradas isoladamente ou simultaneamente.

Deve permitir o bloqueio de vulnerabilidades.

Deve permitir o bloqueio de *exploits* conhecidos.

Deve detectar e bloquear o tráfego de rede que busque acesso a *command and control* e servidores de controle utilizando múltiplas camadas de DNS, *AFC* e firewall.

Deve incluir proteção contra-ataques de negação de serviços.

Ser imune e capaz de impedir ataques básicos como: *SYN flood, ICMP flood, UDP Flood*, etc.

Suportar bloqueio de arquivos por tipo.

Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

Os eventos devem identificar o país de onde partiu a ameaça.

Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.

O equipamento do tipo 1 deve ter a capacidade de atuar como um gateway AntiSpam de modo que possa realizar filtragens dos e-mails e aplicar políticas.

O gateway de e-mail incluso no equipamento do tipo 1 deve ter pelo menos as seguintes proteções:

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Sender Policy Framework (SPF);
Domain Keys Identified Mail (DKIM);
Domain-based Message Authentication, Reporting & Conformance (DMARC);
Bounce Address Tag Validation (BATV);
O filtro de e-mail deve quarentenar os e-mails suspeitos ou realmente maliciosos;
A solução deve possibilitar aos usuários acessarem um painel para verificação da sua caixa pessoal de quarentena, possibilitando então a liberação ou a exclusão das mensagens;
A função de AntiSpam deve permitir a configuração de relays com a possibilidade de autenticação deles;
A função de AntiSpam deve possibilitar também o envio de e-mails seguros, realizando a criptografia das mensagens bem como dos seus anexos.
A função de AntiSpam deve conter funcionalidades de prevenção a perda de dados (DLP) para evitar que informações sigilosas sejam vazadas;
O equipamento deverá possuir firewall de aplicação Web (*WAF*) com a função de *reverse proxy*, função de *URL hardening* realizando *deep-linking* e prevenção dos ataques de *path traversal* ou *directory traversal*.
O firewall de aplicação Web (*WAF*) deverá realizar *cookie signing* com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.
O firewall de aplicação Web (*WAF*) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do *WAF* e permissão e bloqueio de *ranges* de IP.
Deverá permitir a identificação dos IPs de origem através de proxy via “X-forward headers”.
Deve possuir pelo menos duas *engines* de antivírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.
Proteção pelo menos contra os seguintes ataques, mas não limitado a: *SQL injection* e *Cross-site scripting*.

CONTROLE E PROTEÇÃO DE APLICAÇÕES

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, *port hopping* e túnel através de tráfego SSL encriptado.

Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3.

O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algoritmos: curvas elípticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas.

Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website).

Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Atualizar a base de assinaturas de aplicações automaticamente.

Reconhecer aplicações em IPv6.

Limitar a banda usada por aplicações (*traffic shaping*).

Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários.

Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuem acesso a estes aplicativos devem ter a utilização bloqueada.

CONTROLE E PROTEÇÃO WEB

Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, Radius, *E-directory* e base de dados local;

Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius;

Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

Possuir pelo menos 90 categorias de URLs;

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;

Deve ser capaz de forçar as restrições do Youtube

Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;

Suportar a criação categorias de URLs customizadas;

Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada

Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;

Deve realizar caching do conteúdo web;

Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet.

A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual.

A solução deve permitir o enforce dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar.

IDENTIFICAÇÃO DE USUÁRIOS

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).

Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, afim de garantir que usuários logados em servidores de multi sessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas um IP de origem;

Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.

Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

QUALIDADE DE SERVIÇO – QoS

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e *bit rate* de modo individual ou compartilhado.

Suportar priorização *Real-Time* de protocolos de voz (VoIP).

Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP.

REDES VIRTUAIS PRIVADAS – VPN

Suportar VPN *Site-to-Site e Cliente-to-Site*.

Suportar IPsec VPN.

Suportar SSL VPN.

Suportar L2TP e PPTP.

Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.

Deve possuir opção de VPN IPSEC com aplicação nativa do fabricante.

Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1;*Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (*Advanced Encryption Standard*); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.

Deve suportar nativamente a integração com a Amazon, a fim de estabelecer um túnel seguro entre os equipamentos e a VPN da AWS.

Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-Malware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

Suportar autenticação via AD/LDAP, *Token* e base de usuários local;

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Permitir estabelecer um túnel SSL VPN com uma solução de autienticação via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local.

GERÊNCIA ADMINISTRATIVA CENTRALIZADA

Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

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

Estar licenciada para gerenciar as soluções de firewall de próxima geração.

Devem ser fornecidas soluções virtuais, em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação.

Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração, sem necessidade de acesso direto aos equipamentos.

Deve permitir a criação de Templates para configurações.

Deve possuir indicadores do estado de equipamentos e rede.

Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas;

Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

Deve possibilitar o envio dos logs via syslog com conexão segura (TLS).

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS

Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

Estar licenciada para gerenciar as soluções de firewall de próxima geração.

Devem ser fornecidas soluções virtuais, em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 2TB de dados.

Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

Deve possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

Deve conter relatórios pré configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;

Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

Deve conter customizações dos relatórios para inserção de logotipos próprios.

Deve fornecer relatórios de compliance SOX, HIPAA e PCI.

Deve permitir a exportação via PDF ou Excel.

Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

Deve fornecer relatórios de tendências.

Deve fornecer logs em tempo real, de auditoria e arquivados.

Deve possuir mecanismo de procura de logs arquivados.

Deve ter acesso baseado em Web com controles administrativos distintos.

INTEGRAÇÃO COM SOLUÇÃO DE ENDPOINT

A solução de firewall deve possibilitar a integração com a atual solução de Endpoint (Sophos Cloud) instalada no ambiente da contratante.

A integração deve possibilitar a criação de regras de bloqueio de endpoints, com determinado status, dentro do Firewall de forma automática, sem que haja intervenção por parte do time da contratante.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

A integração deverá ser nativa entre o firewall e o endpoint, ou utilizando APIs de integração da solução de firewall.

Caso a integração não seja nativa, cabe a CONTRATADA:

Desenvolver completamente a solução de integração do Firewall e o Endpoint instalado (Sophos Cloud);

O Software de integração deve realizar a criação das regras do Firewall com no máximo 2 (dois) minutos após o incidente detectado no Endpoint;

Possuir interface WEB, acessada por HTTP ou HTTPS, para definição dos objetos das regras a serem criados, com no mínimo origem, destino, status do endpoint e protocolos;

Possibilitar o envio de e-mails sobre as ações do software;

Entregar o software de integração em máquina virtual, Windows ou Linux, juntamente com as devidas licenças necessárias para sistemas operacionais, banco de dados, etc;

A máquina virtual será instada no ambiente da contratante, não sendo permitido soluções em nuvem;

A máquina virtual não deverá ter qualquer acesso remoto que não seja acordado pela contratante;

A mesma não deverá enviar/receber pacotes TCP/UDP ou por qualquer outro meio de comunicação, que não sejam os objetos de Firewall deste edital ou a console do endpoint da contratante;

A gestão do sistema operacional da máquina virtual em questão será de inteira responsabilidade da contratante, de modo a garantir que sejam realizados todos os updates, correções de patchs, segurança do sistema operacional, bem como com seus softwares, alterações de versões, etc;

A máquina virtual deve ser utilizada única e exclusivamente para o fim proposto no edital, não sendo permitido que a máquina virtual realize qualquer outra função;

Permitir backup das configurações do software de integração, possibilitando o restore em outra máquina virtual de forma a não comprometer o ambiente;

Realizar manutenção/alteração total no software de integração, sem custo adicional, durante o período de vigência do suporte do Firewall Tipo 1;

Realizar teste de bancada, a fim de comprovar a efetividade da integração;

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Possuir atendimento 24 horas por dia, 07 dias por semana (24x7), durante todos os dias do ano, inclusive feriados;

O atendimento deve ser realizado por telefone, e-mail, remoto ou on-site (ilimitado);

Apresentar SLA em contrato com os seguintes tempos:

Criticidade Baixa – Tempo de resposta de até 6 horas e até 48 horas para tempo de solução. Os casos definidos com criticidade baixa são: Falha na console de acesso Web do software de integração, alterações no funcionamento da ferramenta mediante solicitação da contratada, falhas no envio de e-mails por parte do software de integração.

Criticidade Média - Tempo de resposta de 4 horas e até 8 horas para tempo de solução. Os casos definidos com criticidade média são: Bloqueios inesperados realizados pelo software de integração, falha na identificação do status dos endpoints, falha no job de backup.

Criticidade Alta – Tempo de resposta de até 2 horas e até 6 horas para tempo de solução. Os casos definidos com criticidade alta são: Sistema operacional da máquina virtual do software de integração inoperante, com problemas durante o boot da VM, qualquer falha no software que comprometa o funcionamento da solução como um todo.

CARACTERÍSTICAS ESPECÍFICAS DO HARDWARE ACCESS POINT (ITEM 3)

Equipamento deve proporcionar o máximo em segurança e desempenho de rede.

Padrão / Normas WLAN: 802.11ax, Wi-Fi 6

Gerenciamento por meio de plataforma central da fabricante e por interface web local.

Indicado para instalação em ambiente fechado.

Deve permitir ser implantado montado em mesa, parede ou teto.

Rádio duplo: 1x 2,4 GHz banda simples e 1x 5 GHz banda simples

Deve possuir ao menos 4 antenas omnidirecionais internas, sendo: 2x antenas 2,4 GHz e 2x antenas 5 GHz.

Deve possuir tecnologia DFS (Dynamic Frequency Selection) para gerenciar o uso de frequências de rádio.

Desempenho: 2x 2:2.

Taxas máximas de transmissão: 2975 Mbps sendo 575 Mbps (2,4 GHz) +2400 Mbps (5 GHz).

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Interfaces: 1x 12V DC-in, 1x porta Gigabit Ethernet com 802.3at PoE+, Console Micro-USB.

Deve ser ter plataforma na nuvem escalonável que permita o gerenciamento remoto.

Deve possuir recurso de resposta a ameaças ativas para isolamento de hosts comprometidos.

Deve possuir portal cativo para acesso de convidados e visitantes.

Deve permitir o gerenciamento centralizado juntamente com o ecossistema completo das soluções de segurança cibernética da fabricante.

Deve permitir Múltiplos SSIDs.

Deve permitir SSIDs com base em tempo (hora do dia, dia da semana).

Deve permitir Balanceamento de carga do cliente.

Deve permitir Seleção automática de canais.

Deve permitir Seleção de largura do canal.

Deve permitir Direção de banda

Deve permitir Airtime Fairness.

Deve permitir Assistente de roaming (802.11r).

Deve permitir Transição rápida (802.11r).

Deve permitir Portal Cativo: Personalização da página inicial (logotipo, nome, mensagem de boas-vindas, termos e condições).

Deve ser Uniusuário MIMO (SU-MIMO) e Multiusuário MIMO (MU-MIMO).

Deve permitir ter os recursos 802.11 avançados como: Coloração BSS (Basic Service Set), Uplink/Downlink OFDMA e TWT (Target Wake Time).

Deve ter os seguintes recursos de Log e Monitoramento: Captura de Pacotes, Logs de auditoria de Syslog, Log e relatórios de eventos (Relatórios de Syslog), Identidade do usuário (Autenticação baseada no usuário), Detecção de AP ilegítimo.

Deve ter os seguintes recursos de autenticação do usuário / dispositivo: WPA3-Personal SAE, WPA3 Enterprise and Enhanced Open (OWE), Autenticação Enterprise (RADIUS), Filtragem de MAC, Senha diária, semanal, mensal, Autenticação de Backend, Voucher com base em tempo e em cota (de dados), Login via rede social, Isolamento de Cliente, Portal Cativo: Jardim Murado, Rede de convidado – modo de ponte.

Deve ter os seguintes recursos de rede: ARP proxy, Suporte a VLAN, Conversão multicast para unicast, Interface LAG (Link Aggregation Group).

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Requisito de energia (PSE) / Potência (máx): 17,5W

Deve ter certificações e conformidades: CB, UL, CE, FCC, ISED, RCM, TEC, EN 60601-1-2 (Diretiva de Equipamentos Médicos).

Deve permitir alimentação elétrica por meio de Power Over Ethernet, padrão 802.3at (Poe +).

O adaptador PoE deve estar incluso como assessório do equipamento.

Padrão PoE mínimo deve ser 30W por porta.

Deve ser fornecido com kit de montagem incluindo: suporte para montagem em parede e teto (barra T de 15/16'' ou 9/16'') e kits para teto plano, plenum e montagem suspensa.

Licenciamento console de controle: Compatível e integrado com o Firewall.

GARANTIA E ASSISTÊNCIA TÉCNICA

A Garantia dos equipamentos fornecidos deverá ser realizada pelo fabricante pelo prazo de 03 (três) anos, com assistência técnica e solução no prazo máximo de 06 (seis) horas, para o lote 01, comprovados através de declaração do fabricante a garantia ofertada.

A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

A assistência técnica dos equipamentos deverá ser executada pelo fabricante ou empresa credenciada pelo mesmo, comprovado através de declaração do fabricante assumindo a assistência técnica durante a garantia e, no caso, de execução por parte de empresa credenciada, indicar a empresa com os correspondentes contatos.

SERVIÇOS

SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E IMPLANTAÇÃO DO FIREWALL E ACCESS POINT

Todos os equipamentos do Lote 1 deverão ser instalados, configurados e ativados pela CONTRATADA nos locais indicados pela Câmara de Itabirito. Os serviços de instalação e configuração da solução poderão ser executados nos seguintes

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

endereços: Sede da Câmara de Itabirito localizada na Av. Queiroz Junior nº 639, Bairro Praia, Itabirito MG. Centro de atendimento ao Cidadão e Gabinete dos Vereadores localizados na rua José Benedito n°189 - 3° andar, bairro Santa Efigênia, Itabirito MG.

A instalação deverá ser previamente agendada com o gestor do contrato e deverá acontecer em dias úteis no horário de 12:00 às 18:00.

A CONTRATADA deverá realizar os serviços de instalação e configuração dos equipamentos e licenciamentos de forma a garantir o seu pleno funcionamento no ambiente tecnológico da Câmara de Itabirito.

O planejamento, instalação, configuração e ativação dos equipamentos deverão ser executados por profissionais qualificados e a empresa deverá ser credenciada pelo fabricante dos equipamentos.

A CONTRATADA deverá garantir todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue.

Todas as configurações serão realizadas em conformidade com a recomendação do fabricante dos equipamentos e softwares da solução existente, boas práticas de implementação recomendada pelo fabricante e os requisitos fornecidos pela Câmara de Itabirito ao ambiente em questão.

Todos os equipamentos adquiridos na solução deverão ser instalados, configurados, testados e integrados na estrutura existente (rede de dados) da Câmara de Itabirito, garantindo assim a total compatibilidade e interoperabilidade de sua infraestrutura.

A contratada deverá realizar as transferências de regras e migrações de parâmetros existentes nos firewalls atuais mediante disponibilização de acesso e acompanhamento técnico da contratante. Os equipamentos firewalls utilizados atualmente no ambiente da contratante são: 1 servidor físico pfSense e 1 Routerboard Mikrotik RB750Gr3, ambos utilizados em topologia bastion host (o firewall está localizado entre a internet e o segmento de rede interna).

Os equipamentos e serviços serão aceitos mediante comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos e a solução se encontre em operação plena. Essa comprovação será realizada por meio de observação direta das características dos equipamentos, consulta à

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

documentação técnica fornecida e verificação dos serviços de instalação e configurações.

A CONTRATADA deverá fornecer catálogos, manuais e/ou prospectos (em formato físico ou digital) de todos os materiais e equipamentos entregues.

Na execução do serviço, deve estar inclusa pela CONTRATADA toda mão de obra necessária para instalação física e configuração dos equipamentos para o funcionamento pleno dos Access Point.

Deve ser realizado pela CONTRATADA toda a estrutura de cabeamento de redes de dados para interligação entre a área de instalação do Access Point e o backbone da Câmara de Itabirito.

A CONTRATADA, se necessário, deverá prover a instalação de pontos de elétrica para a interligação do access point até o quadro de distribuição de energia existente na estrutura da Câmara de Itabirito.

Deve ser fornecido pela CONTRATADA, caso necessário, material para a instalação dos Access Point como buchas, parafusos, conectores, eletrodutos, conduletes, canaletas, tomadas, cabos, caixas sistema x, tampas, espelhos e suportes.

Deve ser providenciado pela contratada qualquer eventual serviço necessário para execução da instalação física dos Access Point como, por exemplo, furos e reparos em alvenarias ou gessos.

Deve incluir a fixação de equipamentos e materiais com o devido acabamento necessário em conformidade com a arquitetura presente no ambiente.

A contratante irá disponibilizar espaço no rack / armário para abrigar o equipamento Hardware Firewall. Caso não haja espaço será fornecido um novo rack / armário pela contratante para ser instalado pela contratada.

Caberá, portanto, a CONTRATADA a execução de todas as atividades, bem como o fornecimento de todos os materiais necessários e suficientes para a instalação e configuração dos equipamentos do lote 1.

A CONTRATADA deverá designar um profissional Técnico Responsável para acompanhar a execução dos serviços desde o planeamento até a implantação da solução.

Após as fases de implantação dos equipamentos, a equipe técnica da CONTRATADA deverá realizar a transferência tecnológica da solução à equipe técnica da Câmara de Itabirito.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

A CONTRATADA deve realizar o teste de funcionamento dos equipamentos, após sua instalação, na presença do contratante.

Todos os serviços de instalação, configuração e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

Durante os primeiros 2 (dois) dias úteis após a instalação e ativação do sistema, a CONTRATADA deverá manter, no mínimo, 01 (um) técnico para a operação assistida e fornecimento de suporte, nas dependências da Câmara de Itabirito, sem custo adicional para a Autarquia.

Caberá à CONTRATADA a realização dos demais serviços necessários ao pleno funcionamento da solução fornecida.

Adicionalmente a CONTRATADA deverá:

Planejar a instalação e implantação da solução e elaborar o cronograma;

Instalar os equipamentos de acordo com a proposta de hardware deste termo;

Implantar o firewall de nova geração, migrar as configurações existentes para o mesmo e vincular ao AD;

Integrar o firewall aos endpoints;

Instalação física e lógica;

Instalar Cabling e alimentação elétrica dos ativos;

Configuração de regras, a serem definidas com o time;

Validações de regras;

Entregar da documentação pertinente: relatório conclusivo com as configurações e parâmetros definidos bem como um resumo de toda a implementação.

Os serviços deverão ser realizados no prazo máximo de 15 (quinze) dias úteis após a data da entrega dos equipamentos.

Realizar o acompanhamento, suporte, e assistência técnica pós instalação por 12 meses, contemplando ajustes de configurações, dúvidas, recuperação de desastres, novas instalações.

Todos os serviços de instalação e configuração deverão ser executados de forma presencial, por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

SERVIÇO DE TREINAMENTO

Deverá ser realizado programa de treinamento, de forma a capacitar os profissionais da Câmara de Itabirito na utilização dos equipamentos e softwares envolvidos na solução ofertada.

A contratada deve realizar treinamento com transferência de conhecimento para no mínimo 2 pessoas com no mínimo de 32 horas (incluídos nessas horas as 16 horas de implantação assistida).

O treinamento deverá abranger todos os equipamentos, componentes e softwares da solução ofertada, em seus aspectos mais relevantes como instalação, configuração e gerenciamento, tomando por base a Documentação do Projeto, e ainda contemplando princípios básicos de funcionamento, noções de manuseio, operação e conservação, principais comandos e procedimentos diários de operação, procedimentos de emergência a serem executados em casos de contingência, geração, emissão e análise de relatórios.

A CONTRATADA fornecerá treinamento aos colaboradores da CONTRATANTE, com instrutor certificado pelo fabricante, buscando garantir a utilização de práticas corretas na operação do ambiente e a correta reação nos casos de incidentes envolvendo os sistemas do Data Center.

O escopo do plano de treinamento para instalação, operação e configuração, gerenciamento centralizado e gerenciamento de relatórios deve prever:

Informativo global dos componentes tecnológicos envolvidos na prestação dos serviços contratados;

Compreensão geral da filosofia de funcionamento e de operação;

Conhecimento e usabilidade dos recursos (hardwares e softwares) envolvidos;

Funcionalidades do Sistema em seus respectivos módulos.

Reinstalação, implantação e configuração dos equipamentos de Firewall e Access Point;

Parametrização, criação de regras, backups, gerenciamento dos equipamentos de Firewall e Access Point;

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Gerenciamento, monitoramento e emissão de relatórios e logs da solução do objeto da contratação.

O treinamento deverá ser ministrado em local, data e horário indicado pela CONTRATANTE, de modo que o aluno possa praticar, ao menos, a configuração, o gerenciamento e a operação dos equipamentos, soluções e softwares que compõem o data center;

A capacitação na solução deverá acontecer no prazo máximo de 30 (trinta) dias após a instalação e configuração dos equipamentos, no local de instalação dos equipamentos.

Todos os serviços de treinamento e transferência de conhecimento técnico deverão ser executados de forma presencial, por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

SERVIÇO DE SUPORTE TÉCNICO

Serviços de suporte técnico deve ser prestado pela contratada. Este serviço se difere da assistência técnica de hardware do fabricante e garantia que estão incluídos na subscrição dos equipamentos.

Durante o período de suporte técnico, a CONTRATANTE poderá solicitar o suporte técnico remoto ou presencial especializado a contratada, com limite de 4 (quatro) visitas presenciais por mês;

A solicitação de suporte técnico por parte da contratada se dará através de abertura de chamado, a ser realizado por, no mínimo, os seguintes meios de comunicação, disponibilizados sempre em idioma português (Brasil):

Ligação telefônica;

Sistema web (website) com autenticação segura (mínimo usuário e senha de acesso);

E-mail corporativo (em caso de indisponibilidade dos meios anteriormente citados);

O suporte técnico deverá estar disponível na modalidade “5x7” (2ª à 6ª, horário comercial);

A CONTRATADA deverá realizar mensalmente manutenções preventivas, inspeções e conferência dos parâmetros dos equipamentos de forma a garantir o pleno

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

funcionamento e assegurar que as configurações de segurança estejam sendo aplicadas conforme critérios definidos durante a implantação.

O suporte deverá respeitar, no mínimo, os seguintes tempos de resposta para os níveis de severidade abaixo:

Crítica: solução inoperante ou falha de grande impacto causando parada na solução - Atendimento em até 2(duas) horas, com solução em até 6 (seis) horas;

Alta: incidentes que causem danos moderados à solução, como lentidão elevada, travamentos, interrupções recorrentes - Atendimento em até 4(quatro) horas, com solução em até 8 (oito) horas;

Baixa ou informativa: incidentes de baixo impacto, como lentidão esporádica, erros em ferramenta de geração de relatórios. Inclui também chamados para esclarecimento de dúvidas sobre a configuração e/ou funcionamento da solução - Para este nível de severidade o tempo de resposta deverá ser de até 2 (dois) dias, em horário comercial.

O serviço de suporte técnico deverá ser realizado pelo período 12 meses, que será contado após a validação pela contratante da entrega dos serviços de instalação (item 4) e serviço de treinamento (item 5) pela contratada.

O serviço de suporte técnico será pago de forma mensal pela contratante sendo dividido por 12 parcelas do valor total proposta pela contratada.

Os serviços de suporte técnico deverão ser executados por especialista (s) técnico (s) certificado (s) nos componentes do fabricante com a devida apresentação de certificado (s) técnico (s) emitido (s) pelo fabricante do (s) produto (s).

SIGILO E PROPRIEDADE DAS INFORMAÇÕES

Todos os direitos autorais dos materiais fornecidos com base neste termo são de propriedade da CONTRATADA, sendo expressamente vedada sua reprodução e divulgação;

A CONTRATADA e todos os funcionários envolvidos no processo de contratação e execução das atividades deverão manter sigilo absoluto sobre quaisquer informações da CONTRATANTE;

É proibida a interceptação de qualquer tráfego oriundo ou destinado à CONTRATANTE sem autorização judicial.

Recebimento

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Os bens/serviços serão recebidos provisoriamente, pelo responsável pelo acompanhamento e fiscalização do contrato, juntamente com a nota fiscal ou instrumento equivalente, no prazo de 05 (cinco) dias.

O recebimento definitivo dos bens/serviços ocorrerá no prazo de até 10 (dez) dias úteis, a contar da efetivação do recebimento provisório, mediante termo detalhado que certifique de que todas as condições estabelecidas foram atendidas.

O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada e por igual período, quando houve necessidade de diligências para aferição do atendimento das exigências contratuais.

Os bens/serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no termo de referência e na proposta, devendo ser substituídos no prazo de 03 (três) dias, a contar da notificação à Contratada, às suas expensas, sem prejuízo da aplicação das penalidades.

No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da lei nº 14.133/2021, comunicando-se à empresa para emissão da Nota fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

Não sendo sanadas as irregularidades pelo contratado, o fiscal do contrato encaminhará o caso à autoridade superior, para procedimentos inerentes à aplicação de penalidades.

O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e segurança dos bens/serviços, nem a ético-profissional, pela perfeita execução do contrato.

Subcontratação

Não será admitida a subcontratação do objeto contratual.

LGPD

A Contratada deverá cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão deste do contrato, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

A Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

Cláusulas Gerais

O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

A contratada deverá atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados.

A Contratada deverá alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.

A Contratada deverá prestar todo esclarecimento ou informação solicitada pela Contratante, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, se for o caso, bem como aos documentos relativos à execução do objeto.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

A Contratada deverá conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos.

A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133/2021.

A contratada não poderá contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do art. 48, parágrafo único, da Lei nº 14.133/21.

A Contratada é obrigada a comunicar a Câmara a ocorrência de qualquer fato ou condição que possa atrasar ou impedir a execução do objeto.

A justificativa de quaisquer atrasos no cumprimento dos prazos previstos acima somente será considerada se apresentada por escrito, e após aprovação da Câmara.

A tolerância com qualquer atraso ou inadimplemento por parte da Contratada não importará, de forma alguma, em alteração contratual ou renovação, podendo a solicitante exercer seus direitos a qualquer tempo.

A Contratada obriga-se a manter, durante toda a vigência do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar à contratante, imediatamente, qualquer alteração que possa comprometer a manutenção do contrato.

A Contratada deverá atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados.

A Contratada deverá responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias, fiscais e comerciais, e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante.

A Contratada deverá cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

A Contratada não permitirá a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

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

A contratada deverá guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133/2021.

A contratada é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

O atraso ou a abstenção pela Contratante, do exercício de quaisquer direitos ou faculdades que lhe assistam em decorrência da lei ou do presente contrato, bem como a eventual tolerância com atrasos no cumprimento das obrigações assumidas pela Contratada não implicarão em novação, não podendo ser interpretados como renúncia a tais direitos ou faculdades, que poderão ser exercidos, a qualquer tempo, a critério exclusivo da Administração.

O Contrato não estabelece qualquer vínculo de natureza empregatícia ou de responsabilidade entre a Contratante e os agentes, prepostos, empregados ou demais pessoas da Contratada designadas para a execução do objeto, sendo a Contratada a única responsável por todas as obrigações e encargos decorrentes das relações de trabalho entre ela e seus profissionais ou contratados, previstos na legislação pátria vigente, seja trabalhista, previdenciária, social, de caráter securitário ou qualquer outra.

4.2- Da Contratante:

A Contratante deverá:

Fornecer a Contratada, tempestivamente, todos os documentos, informações e os meios necessários à execução do objeto contratado, além de se responsabilizar, integralmente, por todas as declarações, documentos e afirmações prestadas ao mesmo;

Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

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

Notificar a Contratada, por escrito, sobre vícios, defeitos ou incorreções verificadas na execução do objeto, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela Contratada;

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

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

Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias;

Comunicar a Contratada para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133/21;

Efetuar o pagamento à Contratada do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

Aplicar à Contratada as sanções previstas na lei e neste Contrato;

Comunicar a Contratada na hipótese de posterior alteração do projeto pela Contratante, no caso do art. 93, §2º, da Lei nº 14.133/21;

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

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 - Do Valor e Condições de Pagamento

5.1- O valor global da contratação é de R$ _____ (extenso).

5.1.1- A Contratante pagará à Contratada em até 10 (dez) dias úteis contados da finalização da liquidação da despesa.

5.1.1.1- Recebida a Nota Fiscal ou documento de cobrança equivalente, a Câmara terá o prazo de até 10 (dez) dias para fins de liquidação.

5.1.1.1.1- Para fins de liquidação, o servidor designado deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais, tais como:
- o prazo de validade;
- a data da emissão;
- os dados do contrato, do objeto a que se pagará e do órgão contratante;
- o período respectivo de execução do contrato;
- o valor a pagar; e

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

- eventual destaque do valor de retenções tributárias cabíveis.

De forma que a referida verificação terá por fim apurar:
- a origem e o objeto do que se deve pagar;
- a importância exata a pagar;
- a quem se deve pagar a importância, para extinguir a obrigação.

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

5.1.3- O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

5.2- A nota fiscal ou documento equivalente deverá ser emitida pela Contratada com o número de inscrição no CNPJ apresentado na documentação e proposta.

5.3- Para qualquer alteração nos dados da Contratada, esta deverá comunicar a Contratante, por escrito, acompanhada dos documentos alterados, no prazo de 30 (trinta) dias antes da emissão da Nota Fiscal.

5.4- A contratada deverá apresentar junto à nota fiscal a comprovação da sua regularidade fiscal e trabalhista, por meio das Certidões de Regularidade municipal, estadual, federal/INSS Unificada, trabalhista e CRF-FGTS.

5.4.1- Constatando-se a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que regularize sua situação ou apresente sua defesa.

5.4.1.1- Não havendo regularização ou sendo a defesa considerada improcedente, a Contratante adotará as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa e, na existência de pagamento a ser efetuado, este será realizado normalmente.

5.5- Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus a Contratante.

5.6- No caso de atraso de pagamento pela Contratante, desde que o Contratado não tenha concorrido de alguma forma para tanto, os valores devidos serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

CLÁUSULA SEXTA - Da Dotação Orçamentária

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

6.1- As despesas inerentes do objeto da presente contratação correrão por conta da dotação abaixo indicada:
01.031.0001 1.001 – Aquisição de Equipamentos e material permanente para uso exclusivo da Câmara Municipal
4.4.90.52.00.00 – Equipamentos e Material Permanente
Ficha 08

01.031.0001 1.001 – Aquisição de Equipamentos e material permanente para uso exclusivo da Câmara Municipal
4.4.90.39.00.00 – Outros serviços de terceiros pessoa jurídica
Ficha 07

01.031.0001 2.006 – Manutenção das Atividades da Câmara Municipal
3.3.90.40.00.00 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica
Ficha 33

CLÁUSULA SÉTIMA - Da Vigência

7.1- O prazo de vigência da contratação é de **12 (doze) meses,** contados da data de sua assinatura, prorrogável por até 05 (cinco) anos, na forma do art. 106 da Lei n° 14.133/2021.

CLÁUSULA OITAVA - Das Sanções

8.1- O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:
a) dar causa à inexecução parcial do contrato;
b) dar causa à inexecução parcial do contrato que cause grave dano à administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) dar causa à inexecução total do contrato;
d) deixar de entregar a documentação exigida;
e) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
f) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
g) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
h) apresentar declaração ou documentação falsa ou prestar declaração falsa durante a licitação ou a execução do contrato;
i) fraudar a licitação ou praticar ato fraudulento na execução do contrato;
j) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
k) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
l) praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, de 1º de agosto de 2013.

8.1.1- Constituem comportamentos que serão enquadrados na letra d, do item 8.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou da execução contratual:

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

a) deixar de entregar documentação exigida no instrumento convocatório;
b) entregar documentação em manifesta desconformidade com as exigências do instrumento convocatório;
c) fazer entrega parcial de documentação exigida no instrumento convocatório;
d) deixar de entregar documentação complementar exigida pelo Agente de contratação ou Pregoeiro, necessária para a comprovação de veracidade e/ou autenticidade de documentação exigida no edital de licitação.
e) deixar de atender a convocações do Agente de Contratação ou pregoeiro durante o trâmite do certame ou atendê-las de forma insatisfatória.

8.1.2- Constituem comportamentos que serão enquadrados na letra e do item 8.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou da execução contratual:
a) não enviar a proposta adequado ao último lance ofertado ou após a negociação;
b) deixar de encaminhar ou encaminhar em manifesta desconformidade com o instrumento convocatório as amostras solicitadas pelo Agente de Contratação ou Pregoeiro;
c) ofertar preço inexequível na formulação da proposta inicial ou na fase de lances;
d) recusar-se a enviar o detalhamento da proposta quando exigível;
e) solicitar a desclassificação após a abertura da sessão do certame;
f) abandonar o certame.

8.1.3- Constituem comportamentos que serão enquadrados na letra f do item 8.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou execução contratual:
a) recursar-se a assinar o contrato ou a ata de registro de preço;
b) recusar-se a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração.

8.1.4- Constituem comportamentos que serão enquadrados na letra j do item 8.1, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou execução contratual, a prática de quaisquer atos direcionados a prejudicar o bom andamento do certame ou do contrato, em especial:
a) agir em concluiu ou em desconformidade com a lei;
b) induzir deliberadamente a erro no julgamento;
c) apresentar amostra falsificada ou deteriorada.

8.2- O licitante ou contratado que incorra nas infrações previstas, garantido o contraditório e a ampla defesa, sujeitar-se-ão às seguintes sanções:
a) advertência;
b) multa;
c) impedimento de licitar e contratar;
d) declaração de inidoneidade para licitar ou contratar.

8.2.1- A aplicação das sanções acima previstas não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

8.2.2- A sanção de **advertência** será aplicável nas hipóteses de inexecução parcial do contrato que não implique em prejuízo ou dano à administração, bem como na

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

hipótese de descumprimento de pequena relevância praticado pelo licitante ou fornecedor e que não justifique imposição de penalidade mais grave.

8.2.3- A sanção de **multa** terá natureza moratória ou compensatória e poderá ser aplicada isolada ou cumulativamente com as demais sanções acima previstas, no caso de cometimento de qualquer das infrações administrativas previstas no item 8.1.

8.2.3.1- A multa moratória será aplicada nas hipóteses de atraso injustificado na execução do contrato.

8.2.3.2- A multa compensatória será aplicada nas hipóteses de descumprimento de obrigações contratuais, sendo estabelecidas em razão do grau de importância da obrigação desatendida, objetivando-se a compensação das eventuais perdas nas quais a Administração tenha incorrido.

8.2.3.3- A multa moratória será de 0,5% (cinco décimos por cento) por dia de atraso na entrega de material ou execução do serviço, recaindo o cálculo sobre o valor da parcela inadimplida até o limite de 30% (trinta por cento) do contrato ou do instrumento equivalente.

8.2.3.4- A aplicação de multa de mora não impedirá que a administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções acima previstas.

8.2.3.5- Poderá ser aplicada multa compensatória de até 3% (três por cento) sobre o valor de referência ao licitante ou contratado que retardar o procedimento de contratação, descumprir preceito normativo ou obrigações assumidas, tais como:

a) tumultuar a sessão pública da licitação;
b) propor recursos manifestamente protelatórios em sede de contratação direta ou de licitação;
c) deixar de providenciar o cadastramento da empresa vencedora da licitação ou da contratação direta junto ao Sistema de Cadastro de Fornecedores dentro do prazo concedido, salvo por motivo justificado e aceito pela administração;
d) deixar de cumprir as exigências de reserva de cargos previstas em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz;
e) deixar de cumprir o modelo de gestão do contrato;
f) deixar de complementar o valor da garantia recolhida após solicitação do contratante;
g) não devolver os valores pagos indevidamente pelo contratante;
h) não manter, durante a execução do contrato, todas as condições exigidas para a habilitação, em caso de licitação, ou para a qualificação, em caso de contratação direta, ou, ainda, quaisquer outras obrigações;
i) deixar de regularizar, no prazo definido pela administração, os documentos exigidos pela legislação para fins de liquidação e pagamento da despesa;
j) manter funcionário sem qualificação para a execução do objeto;
k) utilizar as dependências do contratante para fins diversos do objeto do contrato;
l) deixar de substituir empregado cujo comportamento for incompatível com o interesse público, em especial quando solicitado pela administração;

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

m) deixar de efetuar o pagamento de salários, vale-transporte, vale-refeição, seguros, encargos fiscais e sociais, bem como deixar de arcar com quaisquer outras despesas relacionadas à execução do contrato nas datas avençadas;
n) deixar de apresentar, quando solicitado, documentação fiscal, trabalhista e previdenciária regularizada;
o) deixar de regularizar os documentos fiscais no prazo concedido na hipótese de o licitante ou contratado enquadrar-se como Microempresa, Empresa de Pequeno Porte ou equiparados, nos termos da Lei Complementar Federal nº 123, de 14 de dezembro de 2006;
p) não manter atualizado e-mail para contato, sobretudo dos prepostos, nem informar à gestão e à fiscalização do contrato, no prazo de dois dias úteis, a alteração de endereços, sobretudo quando este ato frustrar a regular notificação de instauração de processo sancionador;
q) subcontratar o objeto ou a execução de serviços em percentual superior ao permitido no edital ou contrato, ou de forma que configure inexistência de condições reais de prestação do serviço ou fornecimento do bem.

8.2.3.6- Poderá ser aplicada multa compensatória de até 5% (cinco por cento) sobre o valor da parcela inadimplida ao licitante ou contratado que entregar o objeto contratual em desacordo com as especificações, condições e qualidade contratadas ou com irregularidades ou defeitos ocultos que o tornem impróprio para o fim a que se destina.

8.2.3.7- Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela administração ao contratado, além da perda desse valor, a diferença poderá ser paga diretamente à administração, descontada da garantia prestada ou cobrada judicialmente.

8.2.3.8- A multa inadimplida poderá ser descontada de pagamento eventualmente devido pela contratante decorrente de outros contratos firmados com a administração municipal.

8.2.4- A sanção de **impedimento de licitar e contratar** com a Administração Pública Municipal será aplicada pelo prazo máximo de três anos, quando não se justificar a imposição de penalidade mais grave, observando-se os parâmetros estabelecidos, aos responsáveis pelas seguintes infrações:
a) dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo: impedimento pelo período de até dois anos;
b) dar causa à inexecução total do contrato: impedimento pelo período de até três anos;
c) deixar de entregar a documentação exigida para o certame: impedimento pelo período de até dois meses;
d) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado: impedimento pelo período de até quatro meses;
e) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta: impedimento pelo período de até seis meses;
f) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado; impedimento pelo período de até um ano.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

8.2.4.1- A aplicação de três sanções de advertência pelo mesmo motivo, em um mesmo contrato, possibilita a aplicação da sanção de impedimento de licitar e contratar.

8.2.5- Será aplicada a sanção de **declaração de inidoneidade** para licitar e contratar com a Administração Pública direta e indireta, de todos os entes federativos, pelo prazo mínimo de três anos e máximo de seis anos, observando-se os parâmetros estabelecidos, aos responsáveis pelas seguintes infrações:

a) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato: até quatro anos;
b) fraudar a licitação ou praticar ato fraudulento na execução do contrato; até seis anos;
c) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; até seis anos;
d) praticar atos ilícitos com vistas a frustrar os objetivos da licitação: até cinco anos;
e) praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846, de 1º de agosto de 2013: até seis anos.

CLÁUSULA NONA - Garantia de Execução

9.1- Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA - Da Extinção

10.1- Constituem motivos para extinção do contrato os casos previstos no art. 137 da lei nº 14.133/2021, a qual será formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa.

10.2- O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto ou será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

10.2.1- Se as obrigações não forem cumpridas no prazo estipulado, a vigência poderá ser prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

10.3- A extinção do contrato poderá ser:
- determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;
- consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;
- determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

10.3.1- A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

10.4- As hipóteses de extinção do contrato por culpa da contratada, previstas nos incisos I, II e IX do art. 137 da Lei nº 14.133/2021, serão formalizadas em processo administrativo próprio de apuração de infração contratual, respeitado o contraditório e a ampla defesa, sem prejuízo das demais sanções previstas em lei.

10.5- Após a conclusão do processo que ensejar a aplicação de sanções e culminar na rescisão contratual, esta se procederá por meio de termo de rescisão contratual unilateral, devidamente assinado pela autoridade competente.

10.6- A extinção do contrato motivada nos incisos III a VII do art. 137 da Lei nº 14.133/2021 serão precedidas de processo administrativo próprio que deverá conter:
I - requerimento informativo da Contratada relatando o ocorrido, com documentos que comprovem o alegado;
II - manifestação técnica da unidade administrativa quando a análise do pedido e dos documentos apresentados para sua comprovação;
III - termo de rescisão que poderá ser unilateral ou consensual, contendo os dispositivos que ensejaram a extinção contratual.

10.7- Nas hipóteses de extinção do contrato previstas no § 2° do art. 137 da Lei n° 14.133/21, a Contratada deverá protocolar o pedido de rescisão devidamente fundamentado, demonstrando por meio de fatos e/ou documentos o alegado.

10.7.1- Enquanto não protocolado o pedido de rescisão contratual nos termos do caput, a contratada deverá manter a execução contratual inalterada.

10.8- Quando a extinção decorrer de culpa exclusiva da Administração, o contratado será ressarcido pelos prejuízos regularmente comprovados que houver sofrido e terá direito a:
I - devolução da garantia;
II - pagamentos devidos pela execução do contrato até a data de extinção;
III - pagamento do custo da desmobilização.

10.9- A Administração terá a opção de extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

10.9.1- A extinção acima mencionada ocorrerá apenas na próxima data de aniversário do contrato e não poderá ocorrer em prazo inferior a 2 (dois) meses, contado da referida data.

CLÁUSULA DÉCIMA-PRIMEIRA - Do Reajuste

11.1- Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.

11.2- Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pela Contratante, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

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

11.3- No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

11.4- Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

11.4.1- Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

11.4.2- Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

11.5- O reajuste será realizado por apostilamento.

CLÁUSULA DÉCIMA-SEGUNDA - Da Anticorrupção

12.1- Na execução do presente contrato é vedado à Contratante e a(o) beneficiário(a) e/ou a empregado seu, e/ou a preposto seu, e/ou a gestor seu:

12.1.1- Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público ou a quem quer que seja, ou a terceira pessoa a ele relacionada;

12.1.2- Criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o presente Contrato;

12.1.3- Obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações do presente Contrato, sem autorização em lei, no edital;

12.1.4- Conhecer e cumprir previstas na Lei nº 12.846/2013, abstendo-se de cometer os atos tendentes a lesar a administração pública e denunciando a prática de irregularidades de que tiver conhecimento, por meio dos canais de denúncia disponíveis na CONTRATANTE;

12.1.5- Manipular ou fraudar o presente Contrato, assim como realizar quaisquerações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº 12.846/2013.

CLÁUSULA DÉCIMA-TERCEIRA - Da Vinculação Contratual

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br

13.1- Este contrato está vinculado de forma total e plena ao Processo Administrativo nº 465/2024, Pregão Eletrônico **nº 10/2024** e à proposta do licitante, que lhe deu causa.

CLÁUSULA DÉCIMA-QUARTA - Dos Casos Omissos

14.1- Os casos omissos serão decididos pela Contratante, segundo as disposições contidas na Lei nº 14.133/2021, no Decreto Municipal nº 14.754/2023 e demais normas aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078/1990 (Código de Defesa do Consumidor) e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA-QUINTA - Do Foro

15.1- Fica eleito o foro da Comarca de Itabirito, Estado de Minas Gerais, para solucionar quaisquer questões oriundas deste contrato.

E, por estarem justas, as partes firmam o presente Contrato em 02 (duas) vias de igual teor e forma, na presença de duas testemunhas abaixo.

Itabirito, _____ de _____ de _____.

CÂMARA MUNICIPAL DE ITABIRITO
ANDERSON MARTINS DA CONCEIÇÃO
Contratante

Contratada

_____ _____

Testemunha
CPF:

Testemunha
CPF:

Av. Queiroz Júnior, 639 - CX Postal 74- CEP: 35.450-228 - Itabirito/MG
Telefax: (31) 3561-1599 - site: www.itabirito.mg.leg.br