



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

ADVERTÊNCIA

A MUNICIPALIDADE de HORTOLÂNDIA adverte a todos os licitantes, que não está hesitando penalizar empresas que descumpram o pactuado.

Solicitamos que as empresas apresentem suas propostas e lances de forma consciente, com a certeza de que poderão entregar os objetos da forma como foi pedido no edital e dentro dos prazos, preços e padrões de qualidade exigidos.

Vale lembrar também que os pedidos de realinhamento de preço são exceções à regra, destinados sempre a situações excepcionalíssimas e somente serão deferidos, se em total consonância com a lei.

Ratificamos, portanto, que as propostas sejam efetivadas de forma séria e consciente, visando evitar problemas, tanto para a administração pública como para as empresas licitantes.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

PREGÃO ELETRÔNICO

06/2026

ÓRGÃO REQUISITANTE

Secretaria Municipal de Planejamento Urbano e Gestão Estratégica

OBJETO

Ata de registro de preços para aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia, de acordo com as especificações contidas no ANEXO II – Termo de referência.

DATA PARA APRESENTAÇÃO DE PROPOSTAS

INICIAL: 19/01/2026 às 08h00 (horário de Brasília)

FINAL: 02/02/2026 às 08h00 (horário de Brasília)

DATA DA SESSÃO PÚBLICA

Dia **02/02/2026 às 08h30** (horário de Brasília)

LOCAL: WWW.BBMNET.COM.BR

CRITÉRIO DE JULGAMENTO

Menor preço global

MODO DE DISPUTA:

Aberto

COTA PREFERENCIAL ME/EPP/EQUIPARADAS

Não



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

MUNICÍPIO DE HORTOLÂNDIA

PREGÃO ELETRÔNICO Nº 06/2026

Edital Nº 06/2026

PROCESSO ADMINISTRATIVO Nº 100876/2025

Torna-se público que o **MUNICÍPIO DE HORTOLÂNDIA**, por meio da **Secretaria Municipal de Administração e Gestão de Pessoal** (Departamento de Suprimentos), sediada na Rua Professora Celina Franceschini Bueno, nº 100, Bairro Jardim Metropolitano, no Município de Hortolândia – SP, após autorização do **Secretário Municipal de Planejamento Urbano e Gestão Estratégica**, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da **Lei nº 14.133, de 2021**, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1 – DO OBJETO

1.1. O objeto da presente licitação é a Ata de registro de preços para aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia, de acordo com as especificações contidas no ANEXO II – Termo de referência, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em lote único, formados por 06 itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

1.3. O preço de referência para a presente contratação está disponível em tabela que acompanha o Termo de referência anexo a este edital.

1.3.1. Os valores referenciados constituem o teto possível para esta contratação. Não sendo possível a negociação para a contratação por valores superiores a este.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

2 – DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Plataforma BBMNET Licitações Eletrônicas da Bolsa Brasileira de Mercadorias, no endereço www.bbmnet.com.br

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, excluía 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 e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

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

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual – MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

2.6. Não poderão disputar esta licitação:

2.6.1. Aquele que não atenda às condições deste edital e seu(s) anexo(s);

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

2.6.3. Empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

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

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

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

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

2.6.8. Agente público do órgão ou entidade licitante;

2.6.9. Pessoas jurídicas reunidas em consórcio;

2.6.10. Sociedade de Propósito Específico (SPE);

2.6.11. Organizações da sociedade civil de interesse público - oscip, atuando nessa condição;

2.6.12. Cooperativas de trabalho;

2.6.13. 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



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

disciplina a matéria, conforme § 1º do art. 9º da lei n.º 14.133, de 2021.

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

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

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

2.10. 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 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3 – DA CONTRATAÇÃO

3.1. A ATA de Registro de Preços, decorrente desta licitação, terá vigência por 12 (doze) meses contados de sua assinatura, podendo ser prorrogada nos termos da legislação vigente.

3.1.1. Se a ATA for prorrogada, os quantitativos **poderão** ser renovados.

3.1.2. Após envio do e-mail contendo a ATA, a licitante terá o prazo de 05 (cinco) dias úteis para devolvê-la assinada.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

3.1.3. A ATA assinada deve ser enviada como resposta ao mesmo e-mail pelo qual foi recebida.

3.1.4. A assinatura poderá ser efetuada de forma digital, mediante certificado digital emitido em âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), nos termos do art. 12, §2º da Lei Federal 14.133/2021.

4 – DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço, conforme o critério de julgamento adotado neste Edital.

4.3. Após a disputa e negociação do preço, o sistema tornará possível ao licitante vencedor que VINCULE os documentos de HABILITAÇÃO exigidos no edital, sob pena de INABILITAÇÃO no certame licitatório.

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

4.4.1. Cumpre plenamente os requisitos de habilitação;

4.4.2. Está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada está em conformidade com o edital e que o valor ofertado 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;

4.4.3. Não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, xxxiii, da constituição;



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

4.4.4. Não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos iii e iv do art. 1º e no inciso iii do art. 5º da constituição federal;

4.4.5. 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.

4.4.6. Cumpre a exigência de garantia de Participação, conforme art. 58 da Lei 14.133, de 2021.

4.5. 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.

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

4.7. A falsidade da declaração de que trata os itens 4.4 a 4.66 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

4.8. 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.

4.9. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, a partir da fase de julgamento e aceitação das propostas.

4.10. 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.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

4.11. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para providências.

4.12. No momento em que declarar que cumpre a exigência de garantia licitante deverá, sob pena de inabilitação, juntar comprovante de prestação de Garantia de Participação (Garantia de Proposta), através do botão “Anexar documento”, nos seguintes termos:

4.12.1. A prestação da garantia de proposta, que trata o art. 58 da Lei nº 14.133/2021, no valor equivalente a 1% do valor estimado para a contratação, sendo o valor da garantia:

a) R\$ 52.049,13.

4.12.2. Em caso de caução em dinheiro, deve transferir o valor para conta vinculada ao Município de Hortolândia.

a) BANCO DO BRASIL - Agência 6983-3 - Conta corrente 107000-2 - MUNICIPIO DE HORTOLÂNDIA.

4.12.3. A Garantia não poderá ter validade inferior a 90 (noventa) dias da abertura do certame.

4.12.4. A Agente de Contratação da presente licitação não se responsabilizará por informações prestadas erroneamente pelas licitantes, enviadas para e-mails diferentes do informado neste instrumento, assim como solicitações realizadas fora do prazo ou sem tempo hábil para análise e produção dos documentos necessários.

4.12.5. A garantia de proposta poderá ser prestada nas modalidades de que trata o § 1º do art. 96 da Lei nº 14.133/2021.

4.12.6. Implicará execução do valor integral da garantia de proposta a recusa em assinar o contrato ou a não apresentação dos documentos para a contratação.

4.12.7. A Garantia será devolvida aos licitantes no prazo de 10 (dez) dias úteis, contado da assinatura do contrato ou da data em que for declarada fracassada a licitação.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

5 – DO PREENCHIMENTO DA PROPOSTA

5.1. As licitações aptas para o recebimento de propostas estão disponíveis na Plataforma BBMNET no menu “**Sala de Disputa**”, no campo das licitações na coluna (menu) da etapa “**Aberto para receber propostas**”.

5.1.1. O licitante interessado poderá utilizar filtros de buscas e selecionar o lote/item de interesse e, posteriormente preencher os campos exigidos no sistema e finalizar no comando “enviar proposta”.

5.1.2. O Acesso para participar das licitações está condicionado ao cadastro prévio do interessado na Plataforma BBMNET Licitações.

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

5.3. 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.

5.4. 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.

5.5. 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.

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

5.7. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, dentro do período em que o sistema esteja aberto para o recebimento de proposta.

5.8. Os documentos de habilitação serão vinculados pelo licitante provisoriamente classificado com o melhor lance/proposta, e não poderão ser excluídos ou alterados, após o prazo estipulado no item 7.1 deste edital.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

5.9. 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.

5.10. O prazo de validade da proposta não será inferior a **90 (noventa)** dias, a contar da data de sua apresentação.

5.11. Eventual sobrepreço ou superfaturamento da proposta ou lance poderá ser objeto de apuração de responsabilidade.

5.12. Quando for exigido pelo Agente de Contratação, o licitante deverá preencher a ficha técnica do produto ou serviços, com as informações adicionais.

5.12.1. O licitante não poderá em hipótese nenhuma se identificar na ficha técnica, sob pena de desclassificação.

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

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

6.2. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a data final para apresentação de propostas. Os documentos de habilitação serão vinculados na fase de Habilitação, somente pelo licitante vencedor.

6.2.1. Será desclassificada a proposta que identifique o licitante.

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

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

6.3. Quando devidamente justificado e autorizado pelo Agente de Contratação, os



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

licitantes poderão alterar a proposta anteriormente inserida no sistema durante a fase de análise de propostas.

6.4. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

6.5. O sistema disponibilizará campo próprio para troca de mensagens entre o Agente de Contratação e os licitantes, bem como as mensagens automáticas enviadas pelo próprio sistema.

6.6. 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.

6.7. O lance deverá ser ofertado pelo valor global.

6.8. A variação mínima entre os lances será de R\$ 100,00

6.9. Para formulação dos lances, serão aceitos valores compostos por até 2 (duas) casas decimais.

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

6.11. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

6.12. O procedimento seguirá de acordo com o **MODO DE DISPUTA ABERTO**.

6.13. Os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.13.1. 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.

6.13.2. 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.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

6.13.3. 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.

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

6.15. Serão aceitos lances inferiores, iguais ou superiores ao lance de menor valor já ofertado.

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

6.17. No caso de desconexão com o Agente de Contratação, no decorrer da etapa competitiva do pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

6.18. Quando a desconexão do sistema eletrônico para o Agente de Contratação persistir por tempo superior a 03 (três) horas, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Agente de Contratação aos participantes, no sítio eletrônico utilizado para divulgação.

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

6.20. Encerrada a etapa de lances, o sistema identificará as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada para o fim de aplicar-se o disposto nos arts. 44 e 45 da lei complementar nº 123, de 2006, regulamentada pelo decreto nº 8.538, de 2015.

6.20.1. 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.

6.20.2. 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,



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

contados após a comunicação automática para tanto.

6.20.3. 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.

6.21. Só poderá haver empate entre propostas iguais (não seguidas de lances).

6.21.1. 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:

- a) Disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;
- b) 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;
- c) Desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;
- d) Desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

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

- a) 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;
- b) Empresas brasileiras;
- c) Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

país;

d) Empresas que comprovem a prática de mitigação, nos termos da lei nº 12.187, de 29 de dezembro de 2009.

6.22. Será desclassificada a proposta vencedora que:

6.22.1. Contiver vícios insanáveis;

6.22.2. Não obedecer às especificações técnicas contidas no termo de referência;

6.22.3. Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.22.4. Não tiverem sua exequibilidade demonstrada, quando exigido pela administração;

6.22.5. Apresentar desconformidade com quaisquer outras exigências deste edital ou seus anexos, desde que insanável.

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

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

a) Que o custo do licitante ultrapassa o valor da proposta; e

b) Inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.24. 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.

6.25. 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



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

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

6.26. 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.

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

6.26.2. 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.

6.27. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo definido para a contratação, o Agente de Contratação poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

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

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

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

6.28. Após a negociação do preço, o Agente de Contratação iniciará a fase de habilitação.

6.29. É de integral responsabilidade dos licitantes acompanhar o chat da sessão, por onde serão realizadas todas as formas de comunicação relativas ao andamento da sessão.

6.29.1. Qualquer eventual prejuízo resultante do não acompanhamento do



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

chat, é de integral responsabilidade do licitante.

6.30. Ao final da fase recursal, os licitantes interessados em assinar a ata SUBSIDIARIAMENTE e nos mesmos valores do vencedor, devem se manifestar, nos termos do art. 82, VII da Lei Federal 14.133/2021.

6.30.1. A manifestação deverá ser realizada via e-mail, ao endereço licitacao@hortolandia.sp.gov.br, com identificação clara do pregão e lote;

6.30.2. A licitante deverá manifestar expressamente sua intenção de fornecer pelo mesmo valor da licitante vencedora, no prazo máximo de 30 (trinta) minutos a contar da divulgação, via chat, do resultado da etapa recursal não cabendo suposições ou interpretações;

6.30.3. No mesmo e-mail, a licitante interessada deverá enviar toda a documentação de habilitação exigida no item 7.

6.30.4. Caso a licitante interessada seja habilitada, toda a documentação de habilitação será anexada à plataforma pelo Agente de Contratação.

7 – DA FASE DE HABILITAÇÃO

7.1. Encerrada a etapa de negociação, será solicitado ao licitante provisoriamente classificado em primeiro lugar que vincule os documentos de habilitação exigidos no edital, em um prazo máximo de 02 (duas) horas, e verificará se atendem às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. Relação de Apenados, mantida pelo Tribunal de Contas do Estado de São Paulo (<https://www.tce.sp.gov.br/pesquisa-relacao-apenados>); e

7.1.2. Certidões negativas referentes a punições vigentes, mantido pela Controladoria Geral da União (<https://certidoes.cgu.gov.br>).

7.2. A consulta aos cadastros será realizada em nome da empresa licitante e também



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei nº 8.429, de 1992.

7.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Agente de Contratação diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput)

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

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

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

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

7.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o Agente de Contratação verificará se faz jus ao benefício, em conformidade com o item 4.66 deste edital.

7.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o Agente de Contratação 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, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

7.7. 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.

7.8. 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.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

7.8.1. 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.

7.9. GARANTIA DE PARTICIPAÇÃO:

7.9.1. Antes de iniciar a análise dos documentos de habilitação, o pregoeiro analisará o comprovante de prestação de Garantia de Participação (Garantia de Proposta), nos termos do item 4.12, apresentado pela licitante habilitada com a melhor proposta.

7.10. HABILITAÇÃO JURÍDICA:

7.10.1. **Ato constitutivo**, estatuto ou contrato social em vigor, ou registro empresarial devidamente registrado. Em se tratando de sociedade por ações, o estatuto social deverá vir acompanhado dos documentos de eleição de seus

7.11. REGULARIDADE FISCAL E TRABALHISTA:

7.11.1. **CNPJ** – Cadastro Nacional de Pessoa Jurídica emitido pelo Ministério da Fazenda, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

7.11.2. Prova de inscrição no **Cadastro de Contribuintes Municipal**, relativo à sede ou domicílio do licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

7.11.3. Certidão de regularidade de débitos tributários mobiliários com a **Fazenda Municipal**, relativo à sede ou domicílio do licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

7.11.4. Prova de Regularidade para com a **Fazenda Nacional**, comprovada mediante fornecimento de Certidão conjunta negativa de débitos relativos a Tributos Federais e a Dívida Ativa da União, e Seguridade Social;



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

7.11.5. FGTS – Prova de regularidade de recolhimento de Fundo de Garantia por Tempo de Serviço – FGTS, mediante a apresentação de Certificado fornecido pela Caixa Econômica Federal;

7.11.6. CNDT – Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, disponível no Portal do Tribunal Superior do Trabalho (www.tst.jus.br/certidao).

7.11.7. Para todas as certidões exigidas para fins de habilitação fiscal, serão aceitas **“Certidões negativas ou certidões positivas com efeitos de negativas”**.

7.12. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

7.12.1. Certidão negativa de feitos sobre Falência, expedida pelo distribuidor da sede da licitante.

7.12.2. Balanço patrimonial e demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de 03 (três) meses da data de apresentação da proposta;

7.12.3. Em se tratando de sociedade constituída há menos de 12 (doze) meses, no exercício social em curso, a empresa deverá apresentar o Balanço de Abertura;

7.12.4. A comprovação da boa situação financeira da empresa, que será calculada a partir das demonstrações financeiras do último exercício social, já exigível e apresentada na forma da Lei, adotando duas casas decimais, deverá seguir o seguinte:

a) Índice de Liquidez Corrente (ILC) igual ou maior que 1,0 (um), obtido pela fórmula: $ILC = AC/PC$;

b) Índice de Liquidez Geral (ILG) igual ou maior que 1,0 (um), obtido



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

pela fórmula: $ILG = (AC + RLP) / (PC + PNC)$;

c) Grau de Endividamento (GE) no máximo igual a 0,50 (zero vírgula cinquenta), obtido pela fórmula: $GE = (PC + PNC) / AT$;

Sendo:

Índice de Liquidez Corrente	=	ativo circulante ÷ passivo circulante
Índice Liquidez Geral	=	(ativo circulante + realizável a longo prazo) ÷ (passivo circulante + exigível a longo prazo)
Grau de Endividamento	=	(passivo circulante + exigível a longo prazo) ÷ ativo total.

7.13. QUALIFICAÇÃO TÉCNICA:

7.13.1. A licitante vencedora deverá apresentar comprovação de aptidão (capacitação técnico-operacional) para o item 1 – Firewall tipo 1, através de atestado de capacidade técnica emitido por pessoas jurídicas de direito privado ou público, demonstrando que a empresa licitante tenha executado serviços similares com o objeto da licitação, em qualquer quantidade. A comprovação técnica será necessária apenas para o item 1.

7.14. VISITA TÉCNICA

7.14.1. Como condição de participação, as licitantes interessadas deverão vistoriar o prédio da Prefeitura do Município de Hortolândia (Paço Municipal de Hortolândia - Palácio dos Migrantes), situado à Rua Professora Celina Franceschini Bueno, número 100 - Jardim Metropolitano - CEP: 13184-792 - Bairro: Jardim Metropolitano - Hortolândia – SP, para conhecimento das condições reais de implantação, integração e funcionamento da solução de segurança de rede de dados (Firewall) no ambiente tecnológico da Prefeitura do Município de



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

Hortolândia.

7.14.2. A visita técnica deverá ser marcada previamente pela licitante, através do telefone(19)3965-1400 ramal 9028, ou email leoniciooliveira@hortolandia.sp.gov.br, com o Sr. Leonicio Ornelas de Oliveira, A visita técnica será de segunda a sexta feira no período das 08h30min às 11h30min e das 13h30min às 16h30min, até o dia anterior ao da sessão licitatória.

7.14.3. O comprovante de visita técnica deverá ser apresentado pela empresa licitante junto com a documentação de habilitação, devidamente assinado e pelo servidor responsável do departamento de T.I, sob pena de inabilitação. A não apresentação da declaração de visita técnica ensejará a inabilitação da LICITANTE.

7.14.4. Na visita técnica as empresas que participarão da licitação deverão verificar as conexões existentes nos equipamentos que gerenciam a rede da prefeitura para que não ocorram divergências nas propostas em relação ao tipo e velocidades das conexões bem como ao fornecimento dos cabos necessários para tais conexões.

7.14.5. A exigência de visita técnica fundamenta-se na necessidade de assegurar que as empresas licitantes conheçam, previamente, as condições reais de implantação, integração e funcionamento da solução de segurança de rede de dados (Firewall) no ambiente tecnológico da Prefeitura Municipal de Hortolândia. Tal medida garante que as propostas apresentadas sejam tecnicamente adequadas, precisas e plenamente exequíveis, mitigando riscos de incompatibilidades, subdimensionamentos, falhas de planejamento ou necessidade de aditivos futuros.

7.14.6. A licitante poderá substituir a Visita Técnica por declaração formal assinada pelo responsável técnico da licitante acerca do conhecimento pleno das condições e peculiaridades da contratação, conforme modelo apresentado no item 09 do Termo de Referência.

7.15. APRESENTAÇÃO DE AMOSTRA



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

7.15.1. A licitante vencedora deverá apresentar documentos comprobatórios, por meio de relatórios ou catálogos, testes de bancada ou demo. Esses relatórios ou catálogos deverão ser apresentados de forma clara e objetiva, demonstrando a conformidade com os requisitos estabelecidos no termo de referência.

7.16. PROPOSTA FINAL:

7.16.1. Após a aprovação de todos os documentos de habilitação, o licitante habilitado deverá inserir em campo próprio do sistema, arquivo contendo sua proposta final, de acordo com o modelo do **ANEXO III**.

7.16.2. Deve ser inserido um arquivo de proposta final para cada Item/Lote cuja licitante tenha se consagrado habilitada.

7.16.3. O prazo para inserção deste arquivo será de duas horas, prorrogável, nas seguintes situações:

7.16.4. Por solicitação do licitante, mediante justificativa aceita pelo agente de contratação; ou

7.16.5. De ofício, a critério do agente de contratação, quando constatado que o prazo estabelecido não é suficiente para o envio dos documentos exigidos no edital para a verificação de conformidade.

7.17. Os documentos exigidos acima serão apresentados por meio eletrônico, via Sistema BBMNET.

7.18. Havendo dúvida sobre a veracidade do documento, será exigida a apresentação dos originais não-digitais.

7.19. Os documentos apresentados para habilitação deverão estar em nome da licitante e, preferencialmente, com o número do CNPJ/MF. Se a licitante for matriz, todos os documentos deverão estar em nome da matriz. Se for filial, todos os documentos deverão estar em nome da filial, exceto aqueles que, pela própria natureza ou determinação legal, forem comprovadamente emitidos apenas em nome da matriz ou cuja validade abranja todos os estabelecimentos da empresa.

7.20. Os documentos devem estar com seu prazo de validade em vigor. Se este



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

prazo não constar de lei específica ou do próprio documento, será considerado o prazo de validade de 180 (cento e oitenta) dias, a partir da data de sua emissão.

7.21. Eventual inabilitação do licitante será considerada para fins de apuração da veracidade das informações prestadas na declaração de cumprimento aos requisitos de habilitação, conforme o art. 63, I, da Lei nº 14.133/2021.

7.22. Na ausência ou invalidade dos documentos de: garantia de participação; habilitação jurídica; regularidade fiscal e trabalhista; qualificação econômico-financeira; qualificação técnica, o Agente de Contratação poderá consultar sítios oficiais de órgãos e entidades emissores de certidões, para verificar as condições de habilitação das licitantes ou facultar a juntada dos documentos faltantes no prazo de 30 (trinta) minutos, a partir da convocação via chat, desde que seja comprovado, que a empresa detenha a condição pré-existente à data e hora da sessão de abertura do certame.

7.23. Finalizado o prazo estipulado no item 7.1, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência:

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

7.23.2. Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.23.3. Na hipótese descrita no item 7.22.

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

7.25. Na hipótese de o licitante não atender às exigências para habilitação, o Agente de Contratação examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

8. DOS RECURSOS



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

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 apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.4. O tempo mínimo para manifestação da intenção de recurso será de 30 minutos.

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

8.6. 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.

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

8.8. 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.

8.9. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

decisão recorrida até que sobrevenha decisão final da autoridade competente.

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

8.11. Os autos do processo permanecerão com vista franqueada aos interessados junto ao departamento de suprimentos, da Prefeitura de Hortolândia, localizado na Rua Professora Celina Franceschini Bueno, nº 100, Bairro Jardim Metropolitano, no Município de Hortolândia – SP, no horário das 08:00 às 17:00 horas.

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. As infrações e sanções administrativas serão consideradas e aplicadas nos termos do Decreto Municipal 5.181 de 24 de janeiro de 2023.

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

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

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

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, através do e-mail: licitacao@hortolandia.sp.gov.br ou através do Sistema BBMNet.

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



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

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. Este edital, bem como a licitação regida por ele, poderá ser anulado, suspensos ou revogados a qualquer tempo, nos termos da Lei federal 14.133/2021.

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

11.3. 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 Agente de Contratação.

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

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

11.6. 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.

11.7. 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.

11.8. 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.

11.9. O desatendimento de exigências formais não essenciais não importará o



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

11.10. O Manual de operações da Plataforma BBMNET Licitações encontra-se disponível aos interessados no Portal www.bbmnet.com.br.

11.11. Dúvidas ou esclarecimentos adicionais sobre o uso da Plataforma BBMNET Licitações podem ser obtidas nos canais de atendimento da Plataforma BBMNET Licitações, por e-mail, whatsapp, telefone e chat disponíveis no Portal www.bbmnet.com.br.

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

11.13. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e no sítio eletrônico oficial da Prefeitura: www.hortolandia.sp.gov.br > Acesso rápido > Licitações.

12. DOS ANEXOS

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

12.2. ANEXO I – Estudo Técnico Preliminar;

12.3. ANEXO II – Termo de Referência;

12.4. ANEXO III – Proposta Final;

12.5. ANEXO IV – Minuta da ATA de Registro de Preços;

12.6. ANEXO V – Minuta de Termo de Contrato;

12.7. ANEXO VI – Termo De Ciência E De Notificação.

Hortolândia, 12 de janeiro de 2026

Secretaria Municipal de Administração e Gestão de Pessoal



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

ANEXO I

ESTUDO TÉCNICO PRELIMINAR

OBJETO : Ata de registro de preços para aquisição de solução de segurança de rede de dados.

1 - NECESSIDADE DA AQUISIÇÃO (I § 1º do Art.18)

A presente contratação visa estabelecer as diretrizes e requisitos para a aquisição de uma solução de firewall para a prefeitura municipal de Hortolândia. Reconhecendo a crescente importância da segurança da informação no contexto atual, a prefeitura de Hortolândia busca fortalecer seus mecanismos de proteção, garantindo a integridade, confidencialidade e disponibilidade de seus sistemas e dados.

Tendo em vista que a prefeitura é constantemente alvo de ataques cibernéticos e que nos últimos meses tivemos uma invasão que quase colocou a prefeitura em paralisação por tempo indeterminado, precisamos com urgência adquirir uma solução que nos garanta segurança em conexões remotas e acessos de internet com garantia e segurança. A solução ainda vai garantir a possibilidade de redundância de conexão de internet em locais externos ao paço municipal que tenham a necessidade de conexão redundante para que os trabalhos não parem com o rompimento de cabeamento de fibra óptica.

Diante do cenário de ameaças cibernéticas em constante evolução, imprescindível que a administração pública adote medidas robustas para salvaguardar suas informações sensíveis e garantir o adequado funcionamento de suas operações. Nesse sentido, a aquisição de uma solução de firewall moderna e eficiente essencial para minimizar riscos, prevenir incidentes de segurança e assegurar a continuidade das atividades institucionais.

O firewall desempenha um papel crucial na proteção dos ativos digitais da prefeitura de Hortolândia, atuando como uma barreira de defesa que controla o fluxo de dados entre redes, monitorando e filtrando o tráfego com base em regras predefinidas. Essa solução tecnológica oferece uma camada adicional de proteção, permitindo o estabelecimento de políticas de segurança rigorosas, a identificação de atividades suspeitas e a prevenção de acessos não autorizados.

A escolha adequada de uma solução de firewall fundamental para garantir que a prefeitura de Hortolândia esteja alinhada as melhores práticas de segurança da informação, bem como as normas e regulamentares vigentes.

Ao adotar uma abordagem abrangente e proativa, a prefeitura reafirma seu compromisso em proteger os dados e a privacidade dos cidadãos, promovendo a confiança e a transparência em suas operações.

Portanto, este Termo de Referência estabelece os critérios técnicos e operacionais necessários para a seleção de uma solução de firewall que atenda aos requisitos específicos da prefeitura de Hortolândia. Busca-se, assim, estabelecer um ambiente seguro e resiliente, capaz de enfrentar as ameaças em constante evolução e garantir a continuidade dos serviços prestados.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

2 - ÁREAS REQUISITANTES

Secretaria Municipal de Governo - Secretaria Municipal de Planejamento urbano e gestão estratégica

Secretaria Municipal de Assuntos Jurídicos - Secretaria Municipal de Administração e Gestão de Pessoas

Secretaria Municipal de Meio Ambiente e Desenvolvimento Sustentável - Secretaria Municipal de Segurança -
Secretaria Municipal de desenvolvimento econômico e Turismo - Secretaria Municipal de Serviços Urbanos - Secretaria
Municipal de Mobilidade Urbana - Secretaria Municipal de Habitação

Secretaria Municipal de Inclusão e Desenvolvimento Social - Secretaria Municipal de Educação, Ciência e Tecnologia

Secretaria Municipal de Obras - Secretaria Municipal de Saúde - Secretaria Municipal de Cultura - Secretaria Municipal
de Esportes e Lazer

3 - PREVISÃO NO PLANO ANUAL DE CONTRATAÇÃO (II § 1º do Art.18)

A presente contratação está prevista no Plano de Contratação Anual 2025(PCA) da Prefeitura do Município de Hortolândia, conforme subitem 9.6 –serviços de Tecnologia da Informação e Comunicação, com

recursos previstos na lei orçamentária anual.

4 - REQUISITOS DA CONTRATAÇÃO (III § 1º do Art.18)

Trata-se da contratação de empresa especializada para o fornecimento de equipamentos e softwares de firewall para segurança e gerenciamento da solução de proteção da rede de dados da prefeitura municipal de Hortolândia. Os equipamentos em questão serão responsáveis pela análise do tráfego de rede de toda a prefeitura municipal de Hortolândia, garantindo assim a segurança da comunicação dos próprios públicos com o paço municipal, garantindo redundância na comunicação entre as unidades de saúde e educação com o datacenter da prefeitura com toda segurança contra vírus, invasões e controle de acessos à internet de forma segura e confiável. Permitirá ainda a comunicação de máquinas pessoais com a rede de dados da prefeitura de forma a garantir a execução de trabalhos de forma remota ou em casos necessários de forma remota com toda segurança local da rede de dados existente, contratada mediante licitação na modalidade Pregão Eletrônico, nos termos da Lei nº. 14.133/2021;

A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante ser empregado como NGFW ou simplesmente FIREWALL;

Todos os modelos de Tipos de Firewalls ofertados, devem ser do mesmo fabricante e compatíveis com todos os itens de gerência centralizada e gerência de relatórios e logs;

Os equipamentos devem ser novos e sem uso anterior. O modelo ofertado deve estar em linha de produção sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada;

Deve implementar em um único dispositivo, de forma integrada, tecnologia de Next Generation Firewall com capacidade para filtro de pacotes, controle de aplicação, VPN IPSec e IPS, prevenção contra ameaças de vírus,



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

spywares e malwares e filtro de conteúdo/URL, além de haver integração com sandbox para prevenção contra ameaças avançadas;

Todos os equipamentos appliances do tipo firewall ofertados, devem possuir homologação da ANATEL, emitida e válida na data da entrega.

Visando estabelecer efetividade de segurança na solução de FIREWALL e assegurar que o fornecedor tenha uma solução já avaliada por órgão terceiro e independente de mercado, o fabricante da solução deverá constar no “Magic Quadrant for Hybrid Mesh Firewall” de 2025.

Requisitos de Suporte, Garantia e Instalação

a) Serviços

- ✓ Instalação, configuração inicial e testes funcionais
- ✓ Entrega de documentação técnica e topologia
- ✓ Treinamento básico à equipe de TI

b) Suporte Técnico

Suporte remoto e telefônico disponibilizado pelo fabricante ou parceiro certificado

Atendimento mínimo:

- ✓ Horas úteis, com opção de ampliação a 24x7 (se aplicável)
- ✓ SLA para correção de falhas críticas: **até 4 horas**

c) Garantia

- ✓ Garantia total do hardware e software durante todo o período contratual
- ✓ Substituição de equipamento com falha sem custos adicionais

Critérios de recebimento

- ✓ Comprovação de funcionamento em ambiente controlado
- ✓ Apresentação de relatórios pós-instalação
- ✓ Validação do throughput e das políticas de segurança configuradas
- ✓ Aceite formal pela área de TI

Conformidade Legal

A contratação observará:

- ✓ Lei nº 14.133/2021
- ✓ Decreto e normativos do município de Hortolândia
- ✓ Demais normas de segurança da informação aplicáveis ao serviço público

A adoção da Ata de Registro de Preços (ARP) para a contratação de solução de segurança de rede, especificamente firewall de próxima geração, justifica-se pelos seguintes fundamentos técnicos, operacionais e administrativos:

Natureza da demanda e variação de consumo

A necessidade de aquisição de equipamentos e serviços de firewall apresenta características de consumo variável, podendo oscilar em função da ampliação da infraestrutura de rede, integração de novos sistemas, aumento do



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

tráfego de dados e adequações de segurança cibernética. Assim, não é possível prever com precisão, no momento da contratação, a quantidade exata de itens a serem adquiridos ao longo do período. Nesse sentido, a adoção da ARP permite flexibilidade e adequação da contratação às necessidades reais, evitando aquisições excessivas ou insuficientes.

Aquisição para atendimento a múltiplas unidades e órgãos

A solução de firewall atenderá diversos setores e unidades administrativas, que compartilham a mesma infraestrutura de TI ou dependem de políticas unificadas de segurança de rede.

Trata-se de uma ata de registro de preços e cada secretaria emitirá seus empenhos conforme disponibilidade financeira de cada secretaria.

A adoção de ata de registro de preços justifica-se pelo seguinte:

Benefícios operacionais e econômicos

A ARP proporciona:

- ✓ **Racionalização dos procedimentos licitatórios**, evitando repetidas licitações para itens de mesmo objeto.
- ✓ **Economia de escala**, permitindo obtenção de preços mais vantajosos.
- ✓ **Maior agilidade de atendimento**, uma vez que a contratação específica ocorre conforme necessidade, por adesão às atas.
- ✓ **Redução de estoques**, evitando imobilização de recursos financeiros e obsolescência tecnológica.

Adequação ao art. 82 da Lei nº 14.133/2021

A adoção de Ata de registro e Preços observa as hipóteses previstas no art. 82, que permite o SRP quando:

- ✓ for conveniente adquirir bens com flutuação de demanda;
- ✓ houver necessidade de contratação frequente;
- ✓ visar atender mais de um órgão;
- ✓ buscar padronização e vantagem econômica.

A aquisição de solução de firewall se enquadra plenamente nessas condições.

Evolução tecnológica rápida e necessidade de atualizações

O mercado de segurança da informação passa por constante evolução. Assim, a adoção da ARP possibilita **atualizações ou ampliações** durante a vigência da ata, de acordo com necessidades que possam surgir em virtude de novas ameaças ou de crescimento da infraestrutura de rede municipal.

Mitigação de riscos e atendimento às boas práticas de segurança

A solução de firewall é um recurso essencial para preservar a integridade, a confidencialidade e a disponibilidade das informações institucionais. A adoção de ARP permite que o órgão mantenha pronta capacidade de reposição, expansão e adequação, reduzindo riscos operacionais e garantindo conformidade com normas de segurança cibernética.

Os pagamentos deverão ser efetuados em 10 (dez) dias, fora a dezena, da data do ateste das notas fiscais/faturas.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

As notas fiscais/fatura deverão ser emitidas para o **MUNICÍPIO DE HORTOLÂNDIA** sob o número de **CNPJ 67.995.027/0001-32**, exceto quando a secretaria requisitante for a **SAÚDE**, sendo que neste caso, as notas fiscais/fatura deverão ser emitidas para o **FUNDO MUNICIPAL DE SAÚDE** sob o número de **CNPJ 13.843.145/0001-04**.

As licenças terão vigência de 60 meses, mas o pagamento das mesmas será de acordo com o quantitativo solicitado, sendo que todas as licenças deverão ser solicitados no prazo máximo de 12 meses, ou seja, durante o período de vigência da ARP. O pagamento dos serviços descritos nos itens 4, 5 e 6 ocorrerão somente após a conclusão dos mesmos e deverão ser executados no período de vigência da ARP.

Adoção do Sistema de Registro de Preços (SRP)

A adoção do Sistema de Registro de Preços para a aquisição de solução de segurança de dados – *Firewall* – mostra-se adequada e vantajosa para a Administração, considerando as características do objeto e a forma de sua contratação.

Primeiramente, trata-se de contratação **por tempo determinado**, cuja necessidade de fornecimento e/ou serviços associados ocorrerá **sob demanda futura**, não sendo possível definir, de forma precisa, o quantitativo exato a ser adquirido no momento inicial. O SRP possibilita maior flexibilidade na gestão contratual, permitindo que as contratações sejam realizadas conforme a efetiva necessidade da Administração, ao longo da vigência da ata, sem a obrigatoriedade de aquisição imediata de todo o quantitativo estimado.

Ademais, a solução de segurança de dados do tipo *Firewall* possui **caráter padronizado**, uma vez que suas especificações técnicas podem ser claramente definidas no termo de referência, com base em padrões de mercado amplamente consolidados. Tal padronização permite a comparação objetiva das propostas, assegurando a isonomia entre os licitantes e a seleção da proposta mais vantajosa.

Ressalta-se, ainda, que o uso do Sistema de Registro de Preços contribui para a **otimização dos recursos públicos**, ao reduzir custos administrativos com a realização de múltiplos procedimentos licitatórios, além de conferir maior agilidade às futuras contratações, especialmente em um contexto de constante evolução das ameaças à segurança da informação.

Dessa forma, considerando a natureza do objeto, a imprevisibilidade da demanda, a contratação por tempo determinado e o caráter padronizado da solução, justifica-se a utilização do Sistema de Registro de Preços para a aquisição da solução de segurança de dados – *Firewall*, em conformidade com a legislação vigente e os princípios da eficiência, economicidade e planejamento.

5 - ESTIMATIVA DE QUANTIDADES E MEMÓRIAS DE CÁLCULO (IV § 1º do Art.18)

Os quantitativos foram estimados levando em considerações os seguintes fatores:

- ✓ Quantidade de locais remotos ao paço municipal necessários para a comunicação com o data center da prefeitura municipal de Hortolândia;
- ✓ Velocidade da conexão de internet contratada pela prefeitura municipal de Hortolândia;
- ✓ Quantidade de próprios públicos que necessitam de redundância de conexão no Município de Hortolândia;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Quantidade de secretarias e usuários que utilizam a rede de dados;

- ✓ Quantidade de e-mails existentes para contas oficiais da prefeitura de Hortolândia;

Todos os requisitos mínimos foram fixados considerando padrões comuns de mercado, apresentado por diversas empresas especializadas neste tipo de solução, de modo a assegurar o atendimento das necessidades da contratação e a manutenção da competitividade do certame.

ITEM	CÓDIGO	QTDE	UN.	DESCRIÇÃO	COTA	MARCA	VALOR UNIT	VALOR TOTAL
01	12.3.3929	02	Un	Firewall tipo 1			978.527,46	1.957.054,92
02	12.3.3930	30	Un	Firewall tipo 2			34.753,68	1.042.610,40
03	12.3.3931	110	Un	Firewall tipo 3			14.498,07	1.594.787,70
04	12.3.3932	01	Un	Solução de Gerenciamento Centralizado e Relatório: NGFW Tipos 1, 2 e 3			132.813,53	132.813,53
05	12.3.3933	70	Un	Solução para acesso seguro à aplicação privada e ZTNA			3.438,35	240.684,50
06	12.3.3939	01	Un	Treinamento para a solução			236.962,00	236.962,00

Os quantitativos estão diretamente relacionados com a quantidade de locais (próprios públicos que a prefeitura possui) pois, em cada local deverá ser instalado um equipamento para proteção da comunicação. Em relação a quantidade de licenças, elas são para acesso remoto seguro e é baseado na quantidade de pessoas que precisam viajar ou participarem de congressos e precisam se conectar a rede da prefeitura de forma segura.

6 - LEVANTAMENTO DE MERCADO

Considerando a importância da segurança de dados em redes de dados da prefeitura municipal de Hortolândia, avaliamos algumas soluções que se baseavam apenas em softwares, mas acabamos verificando que a solução não atendia à todas as necessidades, pois, temos a necessidade de proteger a rede local do paço municipal, mas também as redes que estão nos próprios públicos espalhados pelo município. Temos também a necessidade de acessos remotos em casas de home office ou de alguma viagem de representantes da prefeitura em outras cidades e que neste período de viagem precisam acessar a rede de dados e realizar despachos, assinaturas e demais tarefas do cotidiano de forma segura e sem riscos aos dados existentes e acessados.

Foram realizadas várias pesquisas no mercado e todas apontavam para soluções que integravam hardware e software do mesmo fabricante formando um conjunto eficiente que garante os acessos de forma segura e com velocidade desejada. Existem vários fabricantes que oferecem essas soluções integradas de hardware e software para gerenciamento da solução de segurança da e de de dados da prefeitura municipal de Hortolândia. A melhor forma que entendemos é a aquisição dos equipamentos com a solução de software integrada por um período de 60 meses que faz com que os valores fiquem diluídos no período sendo de grande vantagem financeira e tecnológica para a prefeitura municipal de



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Hortolândia. Então a solução é a contratação por tempo determinado da solução completa de empresas especializadas na segurança de rede de dados com uso de firewall.

7 - JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO A CONTRATAR (V § 1º do Art.18)

Diante dos elementos apresentados, entendemos que a solução integrada entre hardware e software de um mesmo fabricante existente no mercado é a melhor escolha para garantir todos os recursos de segurança necessários para uma rede segura nos dias de hoje. Passamos por tentativas de invasão quase toda semana. Elas ocorrem através de e-mails maliciosos, sites maliciosos que induzem o usuário a cometer aberturas e falhas na segurança de rede de dados. Com a aquisição dessa solução poderemos ter mais tranquilidades nos acessos realizados, pois, a solução consegue verificar em tempo real a ameaça e bloqueá-la antes da sua entrada na rede de dados o que garante que a invasão não ocorra evitando assim prejuízos nos dados da administração pública.

A escolha da solução também se justifica pelo seguinte:

- ✓ Grande possibilidade de custo menor ao longo do tempo, além de uma maior competitividade durante o processamento, com possibilidade de redução do preço final;
- ✓ O desembolso ocorrerá conforme as secretarias desejarem participar da plataforma principalmente nos locais remotos ao do paço municipal, porem todas devem participar de forma ativa na compra da solução principal que compõem a proteção da rede do paço municipal;
- ✓ Os servidores da Prefeitura do Município de Hortolândia poderão trabalhar de forma remota quando necessário, a princípio 50 pessoas e de pois poderão ser adquiridas mais licenças se necessário, para poderem entrar na rede da prefeitura de qualquer local que exista um conexão de internet e trabalhar de forma segura sem os riscos de invasão ou sequestro de dados;

8 - ESTIMATIVAS DE PREÇOS OU PREÇOS REFERENCIAIS (VI § 1º do Art.18)

Nos termos do artigo 24 da Lei federal nº 14.133/21 o orçamento estimado da presente contratação, NÃO tem caráter sigiloso e nos termos do artigo 18, inciso XI, da Lei nº 14.133/2021, a divulgação do orçamento da licitação, se dará no Edital de licitação e na plataforma BBMNET, no momento da divulgação do Edital”

Foi efetuada pesquisa no sistema Banco de preços e pesquisa direta com 03 fornecedores. No sistema “Banco de preços” os itens 4 e 6 não foram encontrados. Os itens 2 e 3 da empresa Interquattri e o item 1 da empresa Telefonica/Vivo foram desprezados, pois os valores eram inconsistentes.

Para a definição dos valores estimados foi utilizada a média dos valores obtidos. A média dos preços coletados tende a refletir melhor o conjunto dos dados obtidos, pois seu valor computa todos os preços coletados.

ITEM	CÓDIGO	QTDE	UN.	DESCRIÇÃO	COTA	MARCA	VALOR UNIT	VALOR TOTAL
01	12.3.3929	02	Un	Firewall tipo 1			978.527,46	1.957.054,92



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

02	12.3.3930	30	Un	Firewall tipo 2			34.753,68	1.042.610,40
03	12.3.3931	110	Un	Firewall tipo 3			14.498,07	1.594.787,70
04	12.3.3932	01	Un	Solução de Gerenciamento Centralizado e Relatório: NGFW Tipos 1, 2 e 3			132.813,53	132.813,53
05	12.3.3933	70	Un	Solução para acesso seguro à aplicação privada e ZTNA			3.438,35	240.684,50
06	12.3.3939	01	Un	Treinamento para a solução			236.962,00	236.962,00

9 - DESCRIÇÃO DA SOLUÇÃO COMO UM TODO (VII § 1º do Art.18)

O presente estudo, visa a contratação de empresa especializada no fornecimento de solução de hardware e software integrados para a segurança de conexão à rede de dados da prefeitura e acesso à internet de forma segura e sem riscos de invasões cibernéticas;

A solução baseada em hardware e software integrados garantem uma melhor performance na proteção de redes de dados evitando invasões de vírus, hackers e o sequestro de dados.

Consiste em dois equipamentos redundantes na base do data center que receberá toda a conexão de internet de todas as máquinas com acesso à rede mundial de computadores. Um deles será um equipamento que ficará processando todas as conexões internas e externas a rede da prefeitura e o outro ficará em espera caso o primeiro falhe, o segundo entrará em ação com todas as soluções de software contratadas não necessitando o licenciamento das duas máquinas ao mesmo tempo o que faz com que a solução fique mais vantajoso para os cofres públicos; Consiste ainda em aquisição de equipamentos e softwares integrados para equipamentos menores que deverão ser instalados em próprios públicos fora do paço municipal para a realização de conexão segura com o equipamento principal do data center que garantirá a segurança da conexão entre os locais remotos e o equipamento principal da rede de dados da prefeitura; Esse conjunto de equipamentos locais e remotos e baseados no mesmo software de ponta à ponta garante toda a segurança na conexão entre as redes da prefeitura e impede a invasão de terceiros mesmo que a tentativa seja por e-mails ou sites maliciosos de forma redundante. Permitirá ainda conexões externas à rede da prefeitura para trabalhos de forma remota com toda a segurança de uma acesso interno da rede de dados, no mínimo 50 acessos pelo equipamento principal.

10 - JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO (VIII § 1º do Art.18)

O parcelamento para essa contratação não será viável porque o parcelamento poderia, ao final do processo licitatório, resultar em várias empresas participando dos mesmos serviços e isso poderia causar um prejuízo técnico além de dificultar a fiscalização e a obtenção de melhor qualidade na prestação dos serviços. Justifica-se o não parcelamento da contratação da solução, conforme as razões a seguir:

Interdependência técnica dos componentes da solução:



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

- ✓ A solução de segurança de rede (firewall) a ser contratada envolve a combinação de hardware, software, licenciamento, serviços de instalação, configuração e suporte técnico. O parcelamento dessa aquisição em partes distintas prejudicaria a integração dos sistemas, comprometendo a funcionalidade e a segurança da rede municipal, além de dificultar o gerenciamento centralizado da infraestrutura de TI.

Risco de incompatibilidade e falhas operacionais:

- ✓ Considerando as especificidades técnicas e as necessidades de alto desempenho do sistema de segurança, a contratação de soluções diferentes, fornecidas por fornecedores distintos, pode resultar em problemas de compatibilidade e integração. A falta de uniformidade nas tecnologias empregadas elevaria o risco de falhas operacionais, o que afetaria diretamente a proteção da rede municipal contra ameaças cibernéticas.

Eficiência na gestão e operação:

- ✓ A contratação de uma solução completa e integrada, fornecida por um único fornecedor, permite uma **gestão mais eficiente** do sistema, com **única responsabilidade** pelo fornecimento, suporte e manutenção. Em caso de problemas técnicos, a Prefeitura terá um ponto único de contato, o que facilita a resolução rápida e eficiente de incidentes.

Garantia de atualizações e conformidade com normas de segurança:

- ✓ A escolha de um fornecedor único assegura que toda a solução seja mantida de acordo com as atualizações de segurança e conformidade exigidas, evitando a fragmentação de versões ou padrões de segurança. Isso é essencial para garantir a proteção dos dados municipais, a privacidade dos cidadãos e a conformidade com a legislação vigente, como a LGPD (Lei Geral de Proteção de Dados).

Continuidade dos serviços essenciais para a população:

- ✓ A solução de firewall tem impacto direto na segurança da rede de dados da Prefeitura do Município de Hortolândia, que suporta os serviços essenciais oferecidos à população. A contratação de uma solução única e integrada garante a continuidade e a estabilidade dos serviços públicos digitais, essenciais para a gestão eficiente da Prefeitura e o atendimento à cidadania.
- ✓ Dessa forma, não é viável parcelar a contratação, pois a fragmentação pode comprometer a integridade da solução e gerar maiores custos, riscos operacionais e administrativos. Sendo assim, justifica-se a contratação de uma solução de segurança de rede (firewall) de forma única e integrada e com critério de julgamento global.

11 - DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS OU FINANCEIROS DISPONÍVEIS (IX § 1º do Art.18)

A presente aquisição de solução de segurança de rede de dados do tipo firewall tem como objetivo fortalecer infraestrutura tecnológica da Prefeitura Municipal de Hortolândia, promovendo maior proteção das informações institucionais, disponibilidade dos sistemas públicos e conformidade com as normas de segurança da informação e de governança digital



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

da Administração Pública.

Considerando o crescimento contínuo dos serviços digitais prestados à população, bem como a necessidade de garantir a integridade e a confidencialidade dos dados sob a guarda do Município, a contratação proposta visa alcançar resultados expressivos em termos de economicidade, eficiência operacional e melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis.

Economicidade

Racionalização de custos com infraestrutura de segurança: A solução integrará diversas funcionalidades (firewall, controle de aplicações, prevenção contra intrusões – IPS, VPN, antivírus de tráfego, filtragem web, entre outras) em uma única plataforma, eliminando a necessidade de múltiplos equipamentos e contratos de manutenção separados.

Redução de custos decorrentes de incidentes de segurança: Com maior capacidade de detecção e mitigação de ameaças, será possível evitar interrupções em serviços essenciais (como sistemas de saúde, educação, arrecadação e atendimento ao cidadão), diminuindo perdas financeiras e operacionais.

Aproveitamento da infraestrutura existente: O novo firewall será integrado à atual rede municipal e aos sistemas de monitoramento, prolongando a vida útil dos ativos tecnológicos e maximizando o retorno sobre os investimentos já realizados.

Aquisição orientada pelo custo-benefício: A análise técnica e de mercado garantirá que a contratação observe o princípio da economicidade, priorizando a solução com melhor desempenho, durabilidade e menor custo.

Melhor aproveitamento dos recursos humanos

Otimização das rotinas da equipe de Tecnologia da Informação: A centralização e automação das tarefas de monitoramento e controle de tráfego de rede reduzirão o tempo gasto com atividades repetitivas e corretivas, liberando a equipe para ações estratégicas e de planejamento.

Facilidade de gestão: A interface unificada de administração do firewall permitirá uma operação mais simples, segura e eficiente, diminuindo a dependência de suporte externo e o risco de falhas humanas.

Capacitação e desenvolvimento técnico: A solução favorecerá o aprimoramento das competências dos servidores municipais da área de TI, fortalecendo a capacidade interna de resposta a incidentes e de gestão de segurança cibernética.

Melhor aproveitamento dos recursos materiais e tecnológicos

Modernização e padronização da infraestrutura de segurança: A substituição de equipamentos antigos e heterogêneos por uma solução integrada e escalável trará ganhos de desempenho, estabilidade e consumo energético.

Escalabilidade e sustentabilidade: O novo firewall deverá permitir expansões futuras (em licenças, módulos ou hardware), acompanhando o crescimento dos serviços digitais municipais sem necessidade de novas contratações imediatas.

Integração com políticas de gestão de ativos e continuidade de serviços públicos: A solução apoiará as diretrizes de transformação digital e governança de TI da Prefeitura, garantindo maior resiliência da rede e continuidade operacional.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Conclusão

A implementação da solução de segurança de rede (firewall) trará ganhos significativos de eficiência administrativa, proteção de dados públicos e sustentabilidade financeira para a Prefeitura Municipal de Hortolândia. Com a modernização da infraestrutura tecnológica, será possível oferecer serviços digitais mais seguros, estáveis e acessíveis à população, reforçando o compromisso do Município com a inovação, a transparência e a boa gestão dos recursos públicos.

12 - MAPEAMENTO DE RISCOS (XII § 1º do Art.18)

O processo de aquisição de solução de segurança de rede (firewall) envolve riscos relacionados ao planejamento, ao procedimento de contratação, à execução contratual e à operação contínua do serviço. Com base na análise realizada, foram identificados riscos capazes de afetar o desempenho, a segurança da informação, a economicidade e a continuidade dos serviços.

O quadro de riscos apresenta a identificação, causas, impactos, probabilidade, impacto, nível e medidas de tratamento aplicáveis. As ações propostas visam reduzir a probabilidade de ocorrência e mitigar eventuais impactos sobre a Administração Pública, assegurando aderência às normas vigentes, eficiência operacional e proteção dos ativos de informação

Objetivo do Mapeamento

Identificar, avaliar e propor medidas de tratamento para riscos associados à aquisição de solução de segurança de rede (firewall), visando assegurar eficiência, continuidade, segurança da informação e aderência às necessidades da Administração Pública.

Escopo da Contratação

Aquisição de **firewall de próxima geração** (NGFW), incluindo suporte, atualizações de segurança, garantia e eventuais serviços de instalação e configuração.

Riscos Identificados, Causas, Impactos e Tratamento

A tabela seguinte organiza os riscos mais comuns:

Riscos Relacionados ao Planejamento da Contratação

Risco 1 – Especificações técnicas incompletas ou inadequadas

Causas: Falta de análise aprofundada da infraestrutura; desconhecimento das demandas de tráfego e segurança; ausência de participação da área técnica.

Impacto: Aquisição de solução incompatível; necessidade de aditivos; falhas de desempenho.

Tratamento:

- ✓ Realização de Estudo Técnico Preliminar (ETP) detalhado;
- ✓ Levantamento de tráfego, topologia e políticas de segurança;
- ✓ Validação pela área de TI.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

✓ Probabilidade: Média

Risco 2 – Não observância dos padrões mínimos e normativos

Causas: Falhas na verificação de requisitos legais, de segurança da informação e normas de TI.

Impacto: Contratação irregular; vulnerabilidades; necessidade de retrabalho.

Tratamento:

- ✓ Conferência com normas da IN 01/2019, LGPD, Decreto de Segurança da Informação;
- ✓ Revisão pela área de governança de TI.

Probabilidade: Média

Riscos Relacionados ao Processo de Aquisição

Risco 3 – Preço estimado inadequado

Causas: Pesquisa de preços insuficiente; valores defasados; uso de fontes não confiáveis.

Impacto: Licitação fracassada ou com sobrepreço.

Tratamento:

- ✓ Utilizar múltiplas fontes: painéis oficiais, contratações similares, portais de compras, fabricantes;
- ✓ Justificar metodologia de estimativa.

Probabilidade: Média

Riscos Técnicos da Solução

Risco 4 – Capacidade de processamento insuficiente

Causas: Subdimensionamento da solução; não consideração de features ativas (IPS, VPN, SSL Inspection).

Impacto: Degradação de desempenho; interrupções; indisponibilidade de serviços.

Tratamento:

- ✓ Análise de tráfego atual + projeção de crescimento;
- ✓ Exigir testes de desempenho certificados (ex.: NSS Labs, ICSA, comparativos independentes);
- ✓ Incluir margem para expansão.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Probabilidade: Alta

Risco 5 – Falha de compatibilidade com a infraestrutura existente

Causas: Solução não compatível com switches, roteadores, autenticação, protocolos.

Impacto: Retrabalho, custos adicionais, atraso na implantação.

Tratamento:

- ✓ Levantamento técnico prévio;
- ✓ Exigir suporte a padrões amplamente usados (BGP, OSPF, RADIUS, LDAP, VLAN, 802.1X, VPNs).

Probabilidade: Média

Risco 6 – Descontinuidade do produto (EoL/EoS)

Causas: Aquisição de equipamento próximo ao fim de vida ou suporte.

Impacto: Vulnerabilidades; necessidade de substituição precoce.

Tratamento:

- ✓ Exigir declaração do fabricante de que o modelo está em ciclo ativo;
- ✓ Garantia mínima de suporte (3–5 anos).

Probabilidade: Baixa

Risco 7 – Riscos de segurança da informação não mitigados

Causas: Recursos de inspeção, IPS, antivírus de tráfego, sandboxing ou filtragem insuficientes.

Impacto: Quebra de sigilo, ataques cibernéticos, indisponibilidade de serviços essenciais.

Tratamento:

- ✓ Exigir NGFW com inspeção profunda, inteligência de ameaças, atualizações diárias;
- ✓ Conformidade com boas práticas (ISO 27001, LGPD);
- ✓ Realização de testes antes da aceitação final.

Probabilidade: Média

Riscos Contratuais e de Execução

Risco 8 – Atraso na entrega ou implantação



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Causas: Fornecedor sem estrutura local; dependência de importação.

Impacto: Prejuízo à continuidade de serviços críticos; descumprimento de planejamento.

Tratamento:

- ✓ Verificar lead-time;
- ✓ Prever penalidades contratuais;
- ✓ Probabilidade: Baixa
- ✓ Permitir entrega parcial e instalação por fases.

Risco 9 – Suporte técnico inadequado

Causas: Fornecedor sem equipe qualificada; SLA mal definido.

Impacto: Paradas prolongadas; falha na resolução de incidentes.

Tratamento:

- ✓ Exigir suporte 24x7 para falhas críticas;
- ✓ Definir SLAs (tempo de resposta e solução);
- ✓ Exigir certificações do fabricante para equipe técnica.
- ✓ Probabilidade: Média

Risco 10 – Indisponibilidade de atualizações e assinaturas

Causas: Falta de renovação; contrato mal estruturado; solução proprietária com altos custos posteriores.

Impacto: Vulnerabilidades, risco de ataques, perda de conformidade.

Tratamento:

- ✓ Incluir licenças, atualizações, IPS, filtragem por todo período contratual;
- ✓ Planejar orçamento para renovações.

Probabilidade: Média

Riscos Operacionais após Implantação

Risco 11 – Configuração inadequada ou insegura

Causas: Falta de documentação; implantação incorreta; ausência de boas práticas.

Impacto: Vazamento de dados; falhas de desempenho; brechas de segurança.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Tratamento:

Exigir hardening documentado;

- ✓ Treinamento da equipe local;
- ✓ Auditorias periódicas de segurança.

Probabilidade: Média

Risco 12 – Dependência excessiva do fornecedor

Causas: Solução complexa, pouco conhecida pela equipe interna.

Impacto: Dificuldade de operação; custos adicionais; risco de paralisação.

Tratamento:

- ✓ Treinamento presencial e remoto;
- ✓ Transferência de conhecimento;
- ✓ Documentação completa entregue no aceite.

Probabilidade: Média

13 - POSSÍVEIS IMPACTOS AMBIENTAIS(XII § 1º do Art.18)

A aquisição de um firewall, por se tratar de equipamento eletrônico de pequeno porte, não gera impactos ambientais significativos durante sua fase de operação, uma vez que sua função é essencialmente lógica (processamento e filtragem de tráfego de rede). No entanto, alguns impactos ambientais potenciais associados ao ciclo de vida do equipamento devem ser considerados:

Geração de resíduos eletroeletrônicos (REEE)

- ✓ Ao final da vida útil, o equipamento pode contribuir para a geração de resíduos que requerem descarte ambientalmente adequado.
- ✓ Componentes como placas eletrônicas, metais e baterias demandam destinação e tratamento conforme normas ambientais e logística reversa.

Consumo de energia elétrica

- ✓ O firewall permanecerá em operação contínua (24/7), o que implica consumo energético.
- ✓ A depender da arquitetura e capacidade, esse consumo pode impactar minimamente a matriz energética da instituição.

Embalagens e materiais de transporte



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

- ✓ A entrega do equipamento envolve o uso de embalagens plásticas, papelão e materiais de proteção, que precisam de descarte adequado para evitar resíduos desnecessários.

Processos produtivos do fabricante (impacto indireto)

- ✓ A fabricação de componentes eletrônicos pode envolver uso de recursos naturais e geração de resíduos, embora tais impactos não sejam diretamente controlados pela Administração Pública.

Medidas de Mitigação

- ✓ Exigir que o fornecedor atenda à Política Nacional de Resíduos Sólidos (PNRS), incluindo logística reversa para o descarte futuro.
- ✓ Preferir equipamentos com eficiência energética comprovada.
- ✓ Assegurar que embalagens sejam adequadamente descartadas e encaminhadas para reciclagem.
- ✓ Priorizar produtos com maior durabilidade, reduzindo necessidade de substituições frequentes.

13 - PROVIDÊNCIAS PARA ADEQUAÇÃO AO AMBIENTE DO ÓRGÃO

As adequações para a implantação da solução serão realizadas na configuração dos equipamentos junto a equipe técnica da prefeitura e mudará um pouco a forma de trabalho da equipe que gerencia os acessos à rede de dados da prefeitura, mas sem afetar o funcionário que utilizará a solução na utilização da rede no dia a dia.

14 - CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES (XI § 1º do Art.18)

Não se faz necessária a realização de contratações correlatas e/ou interdependentes para a viabilidade e contratação desta demanda. Já possuímos o necessário para a implantação do objeto a ser contratado, como por exemplo:

- ✓ Serviço de link de internet / conectividade
- ✓ Infraestrutura de rede local (switches, roteadores, servidores)
- ✓ Serviços de segurança da informação (antivírus e monitoramento de rede)
- ✓ Serviços de backup.

15 - DECLARAÇÃO DE VIABILIDADE OU NÃO DA SOLUÇÃO (XIII § 1º do Art.18)

A Prefeitura Municipal de Hortolândia necessita aprimorar a segurança de sua infraestrutura de rede de dados, visando garantir a proteção das informações institucionais e dos sistemas corporativos frente a ameaças cibernéticas, acessos indevidos e tentativas de invasão.

A atual solução de segurança apresenta limitações quanto à capacidade de inspeção de tráfego, atualização de assinaturas de ameaças e gerenciamento centralizado, o que pode comprometer a disponibilidade e a integridade dos serviços públicos digitais.



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

A viabilidade deste Estudo Técnico Preliminar verifica-se pela economia no valor da aquisição e função de ganho de escala, na eficiência com a diminuição dos custos administrativos e função da redução da fragmentação de processos licitatórios.

A equipe técnica da Prefeitura terá o devido treinamento, incluso no objeto a ser contratado, para realizar a instalação e o gerenciamento básico do firewall, podendo contar com suporte especializado do fornecedor contratado. A implantação será realizada de forma planejada, minimizando impacto sobre os serviços públicos digitais

Diante do acima exposto declaramos viável a aquisição de solução de segurança de rede de dados (firewall), por meio de processo licitatório, visando garantir a continuidade, integridade e segurança das operações de tecnologia da informação da Prefeitura Municipal de Hortolândia.

Atenciosamente,

Leonicio Ornelas de Oliveira

Hemerson D. Laranjeira

Hortolândia, 28 de Agosto de 2025.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA
Secretaria de Planejamento Urbano e Gestão Estratégica
Departamento de Infraestrutura da Tecnologia da Informação

ANEXO II

TERMO DE REFERÊNCIA

1 - OBJETO

Ata de registro de preços para Aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia.

1.1 - OBJETO DETALHADO

Ata de registro de preços para aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia, englobando licenças firewall 1,2 e 3, solução de gerenciamento centralizado e relatórios NGFW tipos 1,2 e 3, solução de acesso seguro à aplicação privada e ZTNA e serviço de treinamento para a solução firewall

1.2 - QUANTITATIVO

ITEM	CÓDIGO	QTDE	UN.	DESCRIÇÃO	COTA	MARCA	VALOR UNIT	VALOR TOTAL
01	12.3.3929	02	Un	Firewall tipo 1	Não se aplica		978.527,46	1.957.054,92
02	12.3.3930	30	Un	Firewall tipo 2	Não se aplica		34.753,68	1.042.610,40
03	12.3.3931	110	Un	Firewall tipo 3	Não se aplica		14.498,07	1.594.787,70
04	12.3.3932	01	Un	Solução de Gerenciamento Centralizado e relatório NGFW Tipos 1, 2 e 3	Não se aplica		132.813,53	132.813,53
05	12.3.3933	70	Un	Solução para acesso seguro à aplicação privada e ZTNA	Não se aplica		3.438,35	240.684,50
06	12.3.3939	01	Serv.	Treinamento para a solução Firewall	Não se aplica		236.962,00	236.962,00



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

1.3 - ESPECIFICAÇÕES GERAIS

A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante ser empregado como NGFW ou simplesmente FIREWALL;

Todos os modelos de Tipos de Firewalls ofertados, devem ser do mesmo fabricante e compatíveis com todos os itens de gerência centralizada e gerência de relatórios e logs;

Os equipamentos devem ser novos e sem uso anterior. O modelo ofertado deve estar em linha de produção sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada;

Deve implementar em um único dispositivo, de forma integrada, tecnologia de Next Generation Firewall com capacidade para filtro de pacotes, controle de aplicação, VPN IPSec e IPS, prevenção contra ameaças de vírus, spywares e malwares e filtro de conteúdo/URL, além de haver integração com sandbox para prevenção contra ameaças avançadas;

Todos os equipamentos appliances do tipo firewall ofertados, devem possuir homologação da ANATEL, emitida e válida na data da entrega.

Visando estabelecer efetividade de segurança na solução de FIREWALL e assegurar que o fornecedor tenha uma solução já avaliada por órgão terceiro e independente de mercado, o fabricante da solução deverá constar no “Magic Quadrant for Hybrid Mesh Firewall” de 2025.

1.3.1 - ITEM 1 - FIREWALL TIPO 1

1.3.1.1 - Características mínimas do equipamento:

Possuir desempenho em modo Threat Protection/Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 30 Gbps;

Possuir desempenho em modo de Inspeção SSL ou TLS mínimo de 16.5 Gbps. Desempenho mínimo de Firewall de 95 Gbps;.

Desempenho mínimo de 40 Gbps de IPS.

Suporte mínimo de 15.000.000 conexões simultâneas/concorrentes

Suporte mínimo de 650.000 novas conexões por segundo;

Deve possuir armazenamento interno de no mínimo 900 GB;

Deve possuir fonte de alimentação redundante (Hot Swap) com chaveamento automático de 100-240 VAC;

Deverá possuir ao menos 2 interfaces 40/100 GbE QSFP28 ou 4 interfaces 25GbE SFP28. Todas populadas com transceivers compatíveis com a tecnologia fornecidas com pathcords ópticos ou cabo DAC para interconexão; Todos fornecidos junto com o equipamento.

Deverá possuir 4 interfaces 10GbE SFP+;

Deverá possuir 1 interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento. A VPN



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Client-to-Site IPsec deve ser licenciada para, no mínimo, 2.000 usuários simultâneos. Deverá suportar 2.000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

Deverá suportar, no mínimo, 29 Gbps de desempenho de VPN IPSEC.

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

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

O Equipamento deverá ser homologado pela ANATEL na data de entrega.

Em caso de falha confirmada no Hardware, um novo equipamento deverá estar à disposição no próximo dia útil;

O licenciamento para todos os serviços do Firewall deverá ser de no mínimo 60 meses. A garantia e suporte do hardware deverá ser de 60 meses no mínimo.

Em relação a tecnologia de gateway antimalware, a solução poderá ter limites de tamanho de inspeção de arquivos configurável ou realizar a inspeção dos arquivos sem limites de tamanho de arquivo.

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

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

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

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

Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes;

Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança;

O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas;

Deve fornecer APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos;

1.3.1.2 - Características diversas:

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

Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec;

Deverá implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

Deverá possuir proteção anti-spoofing;

Suportar protocolos de roteamento RIP, OSPF, OSPFv3, BGP e desejável RIPng;

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

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

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

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

Latência;

Jitter;

Perda de pacotes;

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

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

A solução de SD-WAN deve permitir estratégia de encaminhamento de tráfego com base em aplicações conhecidas, como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook;

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

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

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

Deverá suportar DHCP relay;

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

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

Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer), para usuários da rede, individualmente ou em grupo;



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

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

Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) licenciado. É desejável que a solução possa mitigar ataques DDoS e que o mesmo esteja devidamente licenciado;

Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc; Detectar e bloquear a origem de portscans;

Deve permitir o bloqueio de ataques;

Deve permitir o bloqueio de exploits conhecidos;

O gateway Anti-Malware deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP;

Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL/TLS na versão mínima 1.2, que deverá ser decriptografado de forma transparente à aplicação;

Implementar DSCP (Differentiated Services Code Points);

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

Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço;

Implementar mecanismo de sincronismo de horário através do protocolo NTP; Possuir suporte ao protocolo SNMP versões 2 e 3;

Possuir suporte a log via syslog;

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

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

Para tráfego criptografado TLS versão 1.2 no mínimo, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante; Controle, inspeção e de-criptografia de TLS versão 1.2 no mínimo por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, TLS 1.2 e TLS 1.3;

Deve permitir a funcionalidade de ARP bridging;

Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm"; A solução deve permitir a visualização gráfica das regras de segurança e acesso.

1.3.1.3 - Características de VPN:

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

Suportar algoritmos de criptografia AES 128, AES 256;

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

Diffie-Hellman: Grupo 5 (1536 bits) e Grupo 14 (2048 bits).

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

Autenticação via de túneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site;

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

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

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços.

A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

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

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

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

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

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

Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário; Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

1.3.1.4 - Alta disponibilidade:

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

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

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

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

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

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



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

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

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

A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover.

1.3.1.5 - Controle de ameaças:

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

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

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

Implementar funcionalidade de detecção e bloqueio de “call-backs”;

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

solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP;

Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

Implementar interface CLI segura através do protocolo SSH;

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

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

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

Permitir o bloqueio de malwares (vírus, worms, spyware e etc); A

solução deve ser capaz de proteger contra ataques a DNS;

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

solução deve ser capaz de prevenir acesso a websites maliciosos;

A solução deve ser capaz de realizar inspeção de tráfego TLS versão 1.2 no mínimo e SSH; A

solução deverá receber atualizações de um serviço baseado em cloud;

A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

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

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

A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti-malware-Cloud, para que os



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

mecanismos existentes de verificação sejam ampliados;

A solução deve ser capaz de bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos; A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas;

1.3.1.6 - Proteção contra ataques avançados:

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

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

A solução deve ser capaz de inspecionar o tráfego criptografado TLS versão 1.2 no mínimo e SSH; Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb; Implementar a análise de arquivos maliciosos em ambiente controlado;

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

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

A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas;

Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

Conter ameaças avançadas de dia zero;

Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos; Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

Possuir Anti-malware em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP e IMAP;

Minimizar ameaças de dia zero de forma transparente para o usuário final;

Minimizar ameaças de dia zero através de tecnologias de emulação e código de registro;

Minimizar ameaças de dia zero via tráfego de internet;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo. Minimizar ameaças de dia zero antes da execução e evasão de qualquer código malicioso; Conter e mitigar exploits avançados;

A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-malware(Anti-Vírus e Anti-Spyware) automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;

As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real;

A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering;

A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho;

A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças , com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

Inspeção profunda de memória em tempo real; Inspeção

profunda de pacotes livre de remontagem; Descriptografia e

inspeção TLS versão 1.2 no mínimo; Inteligência e controle

de aplicativos;

Recursos SD-WAN seguros;

Em relação a tecnologia de gateway antimalware, a solução poderá ter limites de tamanho de inspeção de arquivos configurável ou realizar a inspeção dos arquivos sem limites de tamanho de arquivo.

1.3.1.7 - Características de filtro de conteúdo WEB:

Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas;

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

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

Permitir a customização de página de bloqueio;

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

Deve permitir submissão de novos sites para categorização; Permitir a

classificação dinâmica de sites web, URLs e domínios;

Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web; Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana;

1.3.1.8 - Características de autenticação:

Prover autenticação de usuários para os serviços Telnet, FTP, HTTP3 e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;

Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Single Sign On; Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento;

Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW; Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;

Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida; Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

1.3.1.9 - Características de administração:

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

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

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

Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração; Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;

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

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

Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados; Deverá suportar minimamente dois tipos de negação de tráfego nas políticas de firewall:

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

Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento; Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente,



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF;

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

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

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

Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreo das configurações aplicadas no produto;

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

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

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

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

Quantidade: 02 unidades

1.3.2 - ITEM 2 - FIREWALL TIPO 2

1.3.2.1 - Características mínimas do equipamento:

Possuir desempenho em modo Threat Protection/Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 2.2 Gbps;

Possuir desempenho em modo de Inspeção SSL ou TLS mínimo de 800 Mbps.

Desempenho mínimo de Firewall de 4,5 Gbps. Desempenho mínimo de 3 Gbps de IPS;

Suporte mínimo de 1.400.000 conexões simultâneas/concorrentes; Suporte mínimo de 20.000 novas conexões por segundo;

Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC; Deve possuir 4 interfaces 1 GbE padrão RJ-45;

Deve possuir 2 interfaces SFP+ nativas de 10 Gbps. Não serão aceitos conversores óticos-elétricos externos;

Deve ser fornecido 1 Transceiver SFP+ Monomodo de 10Gbps; Deve ser fornecido cordão ótico duplex Monomodo SC/LC; Deve possuir 1 interface do tipo console ou similar RJ45;



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G ou 5G;

A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 10 usuários simultâneos;

O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos; Deve suportar no mínimo 250 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

Deve suportar, no mínimo, 2,1 Gbps de desempenho de VPN IPSEC;

Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante;

A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste tr; Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado;

Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame;

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

O Equipamento deverá ser homologado pela ANATEL na data de entrega;

Em relação a tecnologia de gateway antimalware, a solução poderá ter limites de tamanho de inspeção de arquivos configurável ou realizar a inspeção dos arquivos sem limites de tamanho de arquivo.

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

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

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

Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço;

Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade;

Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes;

Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 60 meses, incluindo garantia e suporte; Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança;

O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas;

Deve fornecer APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

1.3.2.2 - Características diversas:

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

Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPsec (NAT-T) e NAT dentro do tunel IPsec;

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

Deve possuir proteção anti-spoofing;

Suportar protocolos de roteamento RIP, OSPF, OSPFv3, BGP e desejável RIPng;

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

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

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

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

- a) Latência;
- b) Jitter;
- c) Perda de pacotes;

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

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

A solução de SD-WAN deve permitir estratégia de encaminhamento de tráfego com base em aplicações conhecidas, como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook;

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

Deve suportar DHCP relay; Deve ser fornecido 08 Transceivers 25Gbe SFP28 por equipamento;

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

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

Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

p2p (peer-to-peer), para usuários da rede, individualmente ou em grupo;

Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”.

A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso;

Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) licenciado. É desejável que a solução possa mitigar ataques DDoS e que o mesmo esteja devidamente licenciado;

Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc; Detectar e bloquear a origem de portscans;

Deve permitir o bloqueio de ataques;

Deve permitir o bloqueio de exploits conhecidos;

O gateway Anti Vírus deve suportar a análise de pelo menos os protocolos HTTP/HTTPS, FTP, IMAP, e SMTP;

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

Implementar DSCP (Differentiated Services Code Points);

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

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

Implementar mecanismo de sincronismo de horário através do protocolo NTP. Possuir suporte ao protocolo SNMP versões 2 e 3;

Possuir suporte a log via syslog;

Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP;

As configurações de RIP e OSPF devem ser configuradas através da interface gráfica;

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

Para tráfego criptografado TLS versão 1.2 no mínimo, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante; Controle, inspeção e de-criptografia de TLS versão 1.2 no mínimo por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, TLS 1.2 e TLS 1.3;

Deve permitir a funcionalidade de ARP bridging;

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

A solução deve permitir a visualização gráfica das regras de segurança e acesso; A

solução deve permitir a visualização gráfica das regras de segurança e acesso;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

1.3.2.3 - Características de VPN:

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços.

A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

Suportar algoritmos de criptografia AES 128, AES 256;

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

Diffie-Hellman: Grupo 5 (1536 bits) e Grupo 14 (2048 bits);

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

Autenticação via de túneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site; A

solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android;

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

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços.

A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

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

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

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

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

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

Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário; Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

1.3.2.4 - Controle de ameaças:

Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada;

Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança;

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

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

Implementar funcionalidade de detecção e bloqueio de “call-backs”;

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

solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP;

Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

Implementar interface CLI segura através do protocolo SSH;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP;

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

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

Permitir o bloqueio de malwares (vírus, worms, spyware e etc); A

solução deve ser capaz de proteger contra ataques a DNS;

A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico;

A solução deve ser capaz de prevenir acesso a websites maliciosos;

A solução deve ser capaz de realizar inspeção de tráfego TLS versão 1.2 no mínimo e SSH; A solução deverá receber atualizações de um serviço baseado em cloud;

A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

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

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

A solução de Gateway Anti-malware deverá ter a tecnologia complementar de Anti-malware-Cloud, para que os mecanismos existentes de verificação sejam ampliados;

A solução deve bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos;

A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas;

1.3.2.5 - Proteção contra ataques avançados:

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

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

A solução deve ser capaz de inspecionar o tráfego criptografado TLS versão 1.2 no mínimo e SSH; Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb; Implementar a análise de arquivos maliciosos em ambiente controlado;

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

A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas;

Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

Conter ameaças avançadas de dia zero;

Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos; Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real; Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

Possuir Anti Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP e IMAP;

Mitigar ameaças de dia zero de forma transparente para o usuário final;

Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro;

Mitigar ameaças de dia zero via tráfego de internet;

Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança; A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo; Minimizar ameaças de dia zero antes da execução e evasão de qualquer código malicioso; Conter e mitigar exploits avançados;

A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti Vírus e Anti Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;

As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real;

A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering;

A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho;

A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

a) Inspeção profunda de memória em tempo real;

b) Inspeção profunda de pacotes livre de remontagem;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

- c) Descriptografia e inspeção TLS versão 1.2 no mínimo;
- d) Inteligência e controle de aplicativos;
- e) Recursos SD-WAN seguros;

Em relação a tecnologia de gateway antimalware, a solução poderá ter limites de tamanho de inspeção de arquivos configurável ou realizar a inspeção dos arquivos sem limites de tamanho de arquivo.

1.3.2.6 - Características de filtro de conteúdo WEB:

Deve possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas;

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

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

Permitir a customização de página de bloqueio;

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

Deve permitir submissão de novos sites para categorização; Permitir a classificação dinâmica de sitesweb, URLs e domínios;

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

Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web; Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana;

1.3.2.7 - Características de autenticação:

Deve prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;

Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Single Sign On; Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento;

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

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

Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida; Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

1.3.2.8 - Características de administração:

Deve permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração; Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW;

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

Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração; Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;

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

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

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

Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados; Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall:

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

Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento; Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças;

Deve permitir a emissão deste relatório em formato PDF;

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

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

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

Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreamento das configurações aplicadas no produto;

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

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

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



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

diversas;

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

Devem ser fornecidas licenças de gerenciamento unificado baseado em nuvem para cada equipamento por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico;

Quantidade 30 unidades;

1.3.3 -ITEM 3 - FIREWALL - TIPO 3

1.3.3.1 - Características mínimas para o equipamento:

Desempenho em modo Threat Protection/Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 1,1 Gbps;

Desempenho em modo de Inspeção SSL ou TLS mínimo de 750 Mbps. Desempenho mínimo de Firewall de 4 Gbps em IPv4 / IPv6.

Desempenho mínimo de 2.2 Gbps de IPS;

Suporte mínimo de 700.000 conexões simultâneas/concorrentes; Suporte mínimo de 16.000 novas conexões por segundo;

Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC; Deve possuir 4 interfaces 1 GbE padrão RJ-45 e possuir 1 interfaces SFP 1 GbE; Deve ser fornecido 1 transceiver SFP Monomodo;

Deve ser fornecido 1 cordão duplex SC/LC Monomodo; Deve possuir 1 interface do tipo console ou similar; Deve possuir 1 interface USB-A ou USB-C;

A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneo. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 5 usuários simultâneos;

Deve suportar 200 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos; Deve suportar, no mínimo, 1.8 Gbps de desempenho de VPN IPSEC;

Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste tr. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado;

Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame;

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

O Equipamento deverá ser homologado pela ANATEL na data de entrega;

Em relação a tecnologia de gateway antimalware, a solução poderá ter limites de tamanho de inspeção de arquivos configurável ou realizar a inspeção dos arquivos sem limites de tamanho de arquivo.

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões;

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

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

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

Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes;

Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 60 meses, incluindo garantia e suporte;

Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança;

O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas;

Deve fornecer APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos;

1.3.3.2 - Características Diversas :

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

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

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

Deve possuir proteção anti-spoofing;

Suportar protocolos de roteamento RIP, OSPF, OSPFv3, BGP e desejável RIPng;

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

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

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

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

a. Latência;

b. Jitter;

c. Perda de pacotes;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego conforme estratégia de balanceamento utilizando os links pertencentes a esse canal lógico;

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

A solução de SD-WAN deve permitir estratégia de encaminhamento de tráfego com base em aplicações conhecidas, como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook;

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

Deve suportar DHCP relay;

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

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

Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer), para usuários da rede, individualmente ou em grupo;

Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”;

A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso;

Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) licenciado. É desejável que a solução possa mitigar ataques DDoS e que o mesmo esteja devidamente licenciado;

Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc; Detectar e bloquear a origem de portscans;

Deve permitir o bloqueio de ataques;

Deve permitir o bloqueio de exploits conhecidos;

O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP; Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões;

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

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

Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade;

Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes;

Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 60 meses, incluindo garantia e suporte; Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança;

O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas;

Deve fornecer APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos;

1.3.3.3 - Características Diversas:

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

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

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

Deve possuir proteção anti-spoofing;

Suportar protocolos de roteamento RIP, OSPF, OSPFv3, BGP e desejável RIPng;

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

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

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

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

- a) Latência;
- b) Jitter;
- c) Perda de pacotes;

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

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

A solução de SD-WAN deve permitir estratégia de encaminhamento de tráfego com base em aplicações conhecidas, como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Outlook;

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

Deve suportar DHCP relay;

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

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

Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer), para usuários da rede, individualmente ou em grupo;

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

Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) licenciado. É desejável que a solução possa mitigar ataques DDoS e que o mesmo esteja devidamente licenciado;

Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc; Detectar e bloquear a origem de portscans;

Deve permitir o bloqueio de ataques;

Deve permitir o bloqueio de exploits conhecidos;

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

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

Implementar DSCP (Differentiated Services Code Points);

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

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

Implementar mecanismo de sincronismo de horário através do protocolo NTP; Possuir suporte ao protocolo SNMP versões 2 e 3;

Possuir suporte a log via syslog;

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



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

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

Para tráfego criptografado TLS versão 1.2 no mínimo, deve descriptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante; Controle, inspeção e decriptografia de TLS versão 1.2 no mínimo por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, TLS 1.2 e TLS 1.3;

Deve permitir a funcionalidade de ARP bridging;

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

A solução deve permitir a visualização gráfica das regras de segurança e acesso; A

solução deve permitir a visualização gráfica das regras de segurança e acesso;

1.3.3.4 - Características de VPN:

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços.

A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

Suportar algoritmos de criptografia AES 128, AES 256;

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

Diffie-Hellman: Grupo 5 (1536 bits) e Grupo 14 (2048 bits).

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

Autenticação via de túneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site;

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

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

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços.

A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

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

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

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

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

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

Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário; Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

1.3.3.5 - Controle de Ameaças:

Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA
Secretaria de Planejamento Urbano e Gestão Estratégica
Departamento de Infraestrutura da Tecnologia da Informação

criada;

Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança;

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

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

Implementar funcionalidade de detecção e bloqueio de “call-backs”;

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

solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP;

Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

Implementar interface CLI segura através do protocolo SSH;

Possuir Anti Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3 e FTP;

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

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

Permitir o bloqueio de malwares (vírus, worms, spyware e etc); A

solução deve ser capaz de proteger contra ataques a DNS;

A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico;

A solução deve ser capaz de prevenir acesso a websites maliciosos;

A solução deve ser capaz de realizar inspeção de tráfego TLS versão 1.2 no mínimo e SSH; A

solução deverá receber atualizações de um serviço baseado em cloud;

A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

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

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

A solução de Gateway Anti-malware deverá ter a tecnologia complementar de Anti-malware-Cloud, para que os mecanismos existentes de verificação sejam ampliados;

A solução deve bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos;

A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas;

1.3.3.6 - Proteção contra ataques avançados:

A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”;

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

A solução deve ser capaz de inspecionar o tráfego criptografado TLS versão 1.2 no mínimo e SSH; Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

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

Implementar a análise de arquivos maliciosos em ambiente controlado;

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

A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas pelo período mínimo de 5 anos;

A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas pelo período mínimo de 5 anos; Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

Conter ameaças avançadas de dia zero;

Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos; Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP;

Mitigar ameaças de dia zero de forma transparente para o usuário final;

Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro;

Mitigar ameaças de dia zero via tráfego de internet;

Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança; A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo; Minimizar ameaças de dia zero antes da execução e evasão de qualquer código malicioso; Conter e mitigar exploits avançados;

A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-malware(Anti-Vírus e Anti-Spyware) automaticamente, definir URLs não



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;

As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real;

A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering;

A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho;

A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi mecanismos baseado em nuvem, permitindo:

- a) Inspeção profunda de memória em tempo real;
- b) Inspeção profunda de pacotes livre de remontagem;
- c) Descriptografia e inspeção TLS versão 1.2 no mínimo;
- d) Inteligência e controle de aplicativos;
- e) Recursos SD-WAN seguros;

Em relação a tecnologia de gateway antimalware, a solução poderá ter limites de tamanho de inspeção de arquivos configurável ou realizar a inspeção dos arquivos sem limites de tamanho de arquivo.

1.3.3.7 - Características de filtro de conteúdo WEB:

Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas;

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

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

Permitir a customização de página de bloqueio;

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

Deve permitir submissão de novos sites para categorização; Permitir a classificação dinâmica de sitesweb, URLs e domínios;

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

Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web; Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana;

1.3.3.8 - Características de autenticação:



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

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

Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Single Sign On; Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento;

Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW; Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;

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

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

1.3.3.9 - Características de administração:

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

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

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

Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração; Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;

A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo, possibilitando implementar as melhores práticas recomendadas pelo fabricante;

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

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

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

Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;

Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento; Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças;

Deve permitir a emissão deste relatório em formato PDF;

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



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

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

Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML ou CSV:

Máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web); Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreamento das configurações aplicadas no produto;

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

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

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

Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API REST full;

Devem ser fornecidas licenças de gerenciamento unificado baseado em nuvem para cada equipamento por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico;

Quantidade: 110 unidades

1.3.4 – ITEM 4 - Solução de gerenciamento centralizado: NGFW Tipos 1, 2 e 3

A solução de gerenciamento centralizado deve gerenciar todos os NGFW descritos neste memorial; Deverá ser fornecido com software de gerenciamento com as seguintes características:

A solução poderá ser entregue como appliance físico ou appliance virtual, sendo todos do mesmo fabricante dos firewalls, não sendo aceita solução de software livre;

Deve permitir o controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;

Deve dar suporte a organização dos dispositivos administrados por grupos;

Deve ser possível aplicar configurações de forma granular, um firewall, em grupos, ou em todos os firewalls;

Deve mostrar o status dos firewalls (standalone ou em alta disponibilidade) a partir da plataforma de gerenciamento centralizado;

Centralizar a administração de regras e políticas usando uma única interface de gerenciamento; O gerenciamento deve permitir/possuir:

- ✓ Criação e administração de políticas de firewall e controle de aplicação;
- Monitores de logs;
- ✓ Debugging;

Deve permitir acesso concorrente de administradores;

A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL;



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

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

A solução deve possuir tela situacional com todo os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador, nome do Hostname do firewall, número de série, modelo, versão do firmware e status da conectividade do equipamento com a gerência em online ou offline;

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

Deve centralizar a administração de regras e políticas, usando uma única interface de gerenciamento; A solução deve possuir Dashboard com sumario de alertas e informação de status de licença;

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

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

A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão no console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN;

A solução deve permitir a criação de modelos de configuração ou “Templates” para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls

Os modelos de configuração ou “templates” devem suportar configurações de interfaces físicas ou virtuais;

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

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

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

Deverá possibilitar a criação de políticas SD-WAN, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall;

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

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

A solução deverá possuir um dashboard com informações como geolocalização dos Firewalls, status (online/offline), distribuição de tráfego, Top Users, ameaças observadas, aplicações mais usadas, e situação do licenciamento;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Deverá armazenar, pelo menos dos últimos 7 dias, informações como: Top

Aplicações por quantidade de conexões;

Top Usuários por quantidade de dados transferidos;

Top Usuários por quantidade de conexões; Top

Virus;

Top Web Categorias;

Top Endereços por dados transferidos;

Top Endereços por quantidade de conexões; Top

Localizações por dados transferidos;

Top Localizações por quantidade de conexões;

Deverá permitir o agendamento de relatório periódico que contenha informações como: Sumário

Executivo;

Recomendações;

Gráfico de risco do ambiente;

Informações de risco por aplicações;

Informações de Compartilhamento de arquivos ;

Informações de Malwares e Virus;

Mapa com estatísticas de geolocalização;

Estatísticas de utilização:

De sessões por IP;

De Uso de tráfego por IP;

De Usuário por sessão; De

usuário por tráfego;

1.3.4.1 - Solução de Relatórios:

A solução deverá suportar o volume de pelo menos 25Gb de Logs por dia ou por tempo de retenção licenciado para 6 meses com armazenamento local ou em nuvem.

A solução poderá ser entregue como appliance físico ou appliance virtual ou em nuvem, sendo todos do mesmo fabricante dos firewalls, não sendo aceita solução de software livre;

Caso seja entregue em appliance virtual, dever ser compatível com VMware ESXi ou Hyper-V ou proxmox;

A solução deverá permitir visualizar sumário com as informações referentes as principais ameaças protegidas pelos firewalls;

Deverá suportar logs do tipo Netflow, IPFIX ou Syslog, para a gerar reports;

O operador da solução de relatórios poderá ter acesso a informações com buscas por um período pré-definido pela solução (última hora, ontem, última semana e último mês) ou customizados para um período específico definido pelo operador;

A solução deverá prover relatórios referente as atividades dos usuários;

A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações: nome da aplicação, nível de ameaça, quantidade de conexões e quantidade de Megabytes trafegados;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações: endereço IP, quantidade de conexões, Usuário, quantidade de Megabytes traegados e Mac Address de origem;

A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantitativo de acessos e megabytes tranferidos;

A solução deverá permitir o agendamento para envio de relatórios periódicos, em formato PDF;

A solução deverá mostrar dados de uso de VPN, informando no mínimo dados como: IP de origem, usuário, conexões e quantidade de dado trafegado;

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

- a. Lista de eventos correlacionados com opção de navegação "drilldown"; ou
- b. Modo gráfico; ou
- c. Lista de logs

A solução deve possibilitar a criação de relatórios de uso de VPN;

Quantidade: 1 unidade

1.3.5 – ITEM 5 - SOLUÇÃO PARA ACESSO SEGURO À APLICAÇÃO PRIVADA E ZTNA:

A solução de para acesso seguro à aplicação privada e ZTNA, deve ser do mesmo fabricante de SD_WAN para garantir integração e funcionamento;

Fornecimento de licenças para Solução para acesso seguro à aplicação privada e ZTNA, que devem ser parte da solução de FIREWALL ou através de licenças adicionais, válidas por 60 meses, abrangendo no mínimo as seguintes características:

1.3.5.1 - Características gerais:

A solução aqui detalhada deve fornecer acesso menos privilegiado a sites privados, servidores diversos, desktops remotos, bancos de dados, clusters kubernetes, e similares recursos e serviços de rede. Deve também controlar o acesso a aplicativos baseados em navegador e infraestrutura de servidor usando proxy reverso com reconhecimento de identidade.

Todas as funcionalidades deverão ser ofertadas na nuvem como serviço, utilizando um único agente instalado nos dispositivos dos usuário autorizados.

Para soluções que limitem a quantidade de dispositivos associados a cada conta de usuário/acesso e controle de dispositivos, o licenciamento adicional (quando se fizer necessário) deverá considerar pelo menos 3 (três) dispositivos habilitados para cada usuário independente;

A plataforma de segurança deverá ter ponto de presença preferencialmente no Brasil,

O ponto de presença (PoP) deve operar na própria infraestrutura do fabricante. De forma alternativa poderá ser através de provedores de nuvem pública tais como AWS, Microsoft, Google, Oracle

Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto ("open source"). Os elementos ofertados não podem ser customizados;

O agente único a ser instalado nos dispositivos protegidos deve ser compatível com no mínimo os seguintes



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

sistemas operacionais:

- ✓ Windows 10 e 11;
- ✓ Ubuntu 22.04 LTS e 24.04 LTS
- ✓ ChromeOS, versão atual estável.

Toda a solução proposta deverá ser implementada com autenticação dos usuários integrada e suportar aplicações de políticas granulares com base em nome do usuário, departamento e grupos integrados com a plataforma Microsoft EntraID da contratante utilizando protocolo SAML 2.0.;

A determinação do estado de saúde e confiança dos dispositivos deve ocorrer de forma permanente e automática, preservando e aplicando os conceitos de confiança zero. A determinação (ou cálculo) do estado de segurança do dispositivo deve possibilitar que o administrador da plataforma escolha condições de acesso diferentes, nas políticas, com base nessa pontuação de status do dispositivo;

A atuação do agente no dispositivo deve ser automática de acordo com o monitoramento permanente, denegando ou restabelecendo conectividade sem necessidade de intervenção do administrador da plataforma ou do usuário;

A conectividade dos dispositivos utilizados pelos usuários deve ocorrer de maneira transparente, sem a necessidade mandatória por parte do usuário de ativar ou desativar o agente instalado;

Caso a solução utilize o conceito de concentradores VPNaaS (VPN como serviço) para conectividade cifrada entre os dispositivos e a infraestrutura, é permitido aprovisionamento de nós dentro da infraestrutura da contratante;

A solução deverá integrar-se nativamente e enviar em tempo real logs para plataformas de SIEM (Security Information and Event Management) como Splunk, IBM Qradar e MS Sentinel;

A solução deve ser capaz de fornecer a visualização de logs em tempo real para tarefas de investigação e auditoria;

1.3.5.2 - Acesso à aplicações privadas:

A solução deverá fornecer acesso remoto a aplicações e recursos internos da contratante, com segurança, validação de identidade, tunelamento encriptado, segregação de aplicações, verificação de postura e conexão direta com privilégio mínimo;

Estes acessos devem ser monitorados permanentemente e de acordo com as políticas granulares de admissão e acesso provisionadas pelo administrador da plataforma;

A solução deve habilitar arquitetura de privilégio mínimo de acesso à rede (Zero Trust Network Access, ZTNA), definindo políticas de acesso granulares para fornecer aos usuários, de acordo com seu contexto, acesso menos privilegiado aos aplicativos ou recursos de forma a reduzir a superfície de ataque;

A solução deve ser ofertada em nuvem, conforme desenhado no modelo SSE (Secure Service Edge), ou no Modelo de Gerencia de Endpoint de Segurança.

Caso utilize, o componente chamado de conector deverá permitir, mas não ser limitado a:

Caso utilize conector, arquitetura de alta disponibilidade e realizar o balanceamento de carga automaticamente, sem depender de nenhum componente de rede da infraestrutura da contratante;

Caso utilize conector, não apresentar superfície de ataque exposta na Internet, sem endereços IP publicamente divulgados;



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Caso utilize, todo tunelamento com os conectores deve ser iniciado por estes (outbound), destinado à nuvem do fabricante onde se concentra o serviço;

Caso utilize conectores, não serão aceitos tunelamentos iniciados pela nuvem em direção aos mesmos;

Caso utilize, permitir que o conector seja instalado de forma flexível à partir de qualquer ponto da rede da contratante, como por exemplo através de NAT (Network Address Translation) disponibilizado no perímetro de acesso à rede interna;

Caso utilize, não deve determinar um ponto único de conexão com a rede da contratante, sendo possível a implementação de múltiplos conectores em pontos da rede, datacenters, ou nuvens privadas distintas, fornecendo ao usuário o acesso direto aos recursos com menor latência possível e de forma dinâmica;

Caso utilize, permitir ao usuário conectar-se a aplicações distintas simultaneamente utilizando conectores em pontos de rede distintos. Estas conexões devem ser determinadas pelas políticas de acesso definidas pelo administrador;

Caso utilize, os conectores devem ser independentes, sem exigência de conectividade interna completa a todos os recursos privados, possibilitando fornecer acesso a aplicações ou recursos simultaneamente aos usuários em múltiplos datacenters ou nuvem, mesmo que estes datacenters ou nuvem não tenham conectividade pré-estabelecida entre eles;

A solução deverá autenticar o usuário em provedor de identidade (IdP) identidade, ofertando políticas granulares, segmentação de aplicações e posturas específicas;

Deve fornecer acesso a aplicações Web, ou qualquer outra com protocolo TCP e UDP, tais como (SSH, RDP, SQL, aplicações cliente-servidor, compartilhamento de arquivos, etc) de forma transparente, sem a necessidade de alteração do cliente original da aplicação, criando tunelamento encriptado que conectará o usuário até a aplicação e não a rede da contratante;

A solução não deve operar como uma VPN tradicional que fornece endereçamento IP da rede local, mas sim conectar o usuário diretamente, após validação de política de identidade, postura e políticas de acesso, aos recursos e aplicações através de tunelamento cifrado específico;

Os usuários remotos não devem possuir visibilidade de aplicativos não autorizados, deve ser preservado o conceito de confiança zero;

Os recursos não autorizados não devem apenas ser inacessíveis, mas também invisíveis aos dispositivos que executam o acesso à rede;

O acesso às aplicações deve ser oferecido minimamente através das seguintes opções: Menu de aplicações publicado no agente instalado no dispositivo;

Acesso direto e transparente após conexão do dispositivo à nuvem de verificação de postura de segurança;

A definição de aplicações, ou segmentos de aplicações, deverá ter a flexibilidade de suportar hostname (FQDN), endereço IP ou domínio com wildcard;

A solução deve fazer com que cada solicitação do usuário flua por meio de políticas contextual para autenticação e autorização consistentes, além de fornecer um ponto de monitoramento e registro unificado;

A solução deve ser protegida contra ataques do tipo “Man-in-the-middle”(MITM);

Deve suportar criptografia dupla dentro dos tuneis encriptados;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

A solução deve permitir o acesso a quais recursos por meio de estrutura básica de políticas que levem em consideração qualquer atributo do usuário fornecido pelo IdP, inclusive customizados, e o estado contextual do dispositivo;

A solução deve trazer o monitoramento da atividade dos usuários, dando às equipes de TI opções de monitoramento e gerenciamento facilitados a todas as atividades de forma granular, entendendo quais usuários, quando, quais aplicações, e quais políticas autorizaram ou denegaram acesso, considerando status de postura e localização do usuário e seu dispositivo;

A solução deve usar console baseado na Web para criar e editar políticas; O portal de gestão central deve trazer:

- ✓ Controle de acesso centralizado;
- ✓ Gestão e políticas;
- ✓ Configuração de postura;
- ✓ Registro de atividades detalhados e seus metadados como usuário, localidade, postura, endereço IP de origem, aplicação destino, política de acesso que concedeu ou denegou acesso;
- ✓ Status da estrutura que suporte a solução e seus conectores;
- ✓ Status das aplicações que deverão ser monitoradas, informando sua disponibilidade ou não;
- Gerenciar a segmentação de acessos ou recursos;
- ✓ Suportar a configuração de qualquer aplicação TCP ou UDP com tráfego originado pelo usuário de forma transparente, sem nenhuma alteração ou customização no cliente original;
- ✓ Permitir o agrupamento de aplicações ou recursos para facilitar a criação de políticas (Ex: Aplicações Administrativas);
- ✓ A solução deverá suportar diferentes tipos de validação de postura;

O suporte a cada tipo pode variar dependendo da plataforma (Windows, Mac, Linux), sendo requerido que no mínimo deverá suportar 2 dos tipos abaixo por plataforma:

- ✓ Validação da presença de um Antivírus;
- ✓ Validação de Certificado Cliente (chave privada e pública) assinada por um CA específico;
- Validação de Certificado confiável no dispositivo;
- ✓ Validação de máquina no domínio;
- Validação de disco cifrado;
- ✓ Validação de Registro de chave no Windows;
- Validação de presença de um arquivo;
- ✓ Exigência de uma versão mínima do Sistema Operacional;

A solução deverá ter mecanismos de proteção e políticas granulares de postura para cada acesso à aplicação, preservando o conceito de confiança zero, permitindo oferecer e impor maiores restrições a aplicações mais críticas, e menos restritas a aplicações consideradas menor críticas pelo administrador da plataforma. Ex.: para acessar a aplicação “A” da CONTRATANTE é necessário estar autenticado, ser parte de grupo pré-determinado de usuários, ter Anti-Virus ativo no dispositivo, ter certificado da contratante presente no dispositivo, e ser parte do domínio de AD;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Para acessar a aplicação “B” será exigido apenas estar autenticado;

A solução deverá também oferecer na mesma plataforma, sem necessidade de instalação de componentes adicionais, o suporte a usuários sem o uso de agentes para fornecer acesso a aplicações privadas através de navegadores Web utilizando extensões plenamente suportadas pelo fabricante da solução;

Deverão ser suportados minimamente os seguintes navegadores:

Google Chrome;

MS Edge; Firefox;

No caso de acesso sem o uso de agentes, o IdP (Identity Provider) deverá ser utilizado para validar a identidade do usuário antes de fornecer qualquer tipo de conectividade via Proxy Reverso ou similar com a aplicação Web privada; A solução deve permitir integração ativa com soluções de NGAV (Next-Gen Anti-Virus) para monitoramento de vetores de ataque nos dispositivos, com atuação concatenada revogando e restabelecendo conectividade de acordo com a integração dinâmica dos dois componentes;

Esta integração ativa com soluções NGAV deve ser integrado ao agente da plataforma de ZTNA, sem necessidade de licenciamento complementar;

Para este quesito de integração ativa com soluções NGAV serão aceitas composições com produtos de fornecedores diferentes;

1.3.5.3 - Proteção contra ameaças WEB, filtros DNS e navegação WEB:

Deverá possuir as seguintes características:

Proteção de camada de DNS e Navegação WEB Segura nos dispositivos minimamente para, mas não limitada a, Windows e MacOS. A solução deve proteger os usuários de sites maliciosos, ransomware ou ataques de phishing filtrando domínios e URLs. A filtragem da Web e proteção contra ameaças tanto no lado do cliente quanto no lado do servidor para desempenho ideal deve ser o quesito fundamental desta funcionalidade.

Proteção contra “DNS Spoofing”. A resolução de DNS deve ser protegida e executada através dos componentes da solução possibilitando o uso de, mas não limitada a, os seguintes componentes: Resolução através do serviço de DNS central da plataforma (nuvem do fabricante da solução);

Resolução através do conector instalado na infraestrutura da contratante; Resolução pelo próprio agente instalado no dispositivo;

Deve oferecer categorização de conteúdo para controle e proteção granular a localidades web acessadas pelos usuários (URLs);

A categorização deve ser provida, permanentemente atualizada e gerenciada pelo provedor da solução; Deve permitir o uso de wildcards (*) nas políticas de acesso. Ex.: deve ser capaz de identificar e categorizar “portal.com.br” e “*.portal.com.br”;

Políticas devem ser passíveis de aplicação a perfis de acesso diferentes, considerando usuários, dispositivos, contexto de utilização, ou qualquer combinação dos itens mencionados;

Deve possibilitar configurações de listas personalizadas de bloqueio e exceções (White/black lists) que se sobreponham às categorizações oferecidas pela plataforma;

1.3.5.4 - Proteção de aplicações públicas (SaaS - CASB (Cloud Access Security Broker):



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

A plataforma deve prover controle de acesso e a sobreposição de segurança para aplicativos SaaS. O CASB deve fornecer visibilidade não apenas para quais aplicativos SaaS os usuários estão acessando, mas também para o que os usuários estão fazendo dentro do aplicativo SaaS. Deve possibilitar uma camada de segurança de confiança de dispositivo sem atrito para login único existente, eliminando riscos associados a ataques de phishing e invasão de contas.

A solução deve incluir proteção para aplicações públicas em nuvem do tipo “SaaS” (Software as a Service) minimamente para, mas não limitada a, dispositivos do tipo Windows ou MacOS.

Deve possibilitar o uso da plataforma em modo proxy, onde seja permitido determinar pelo menos os modos de operação a seguir:

Lista permitida de endereços IP: acessos serão permitidos apenas se originados à partir de origens (endereços IP) previamente determinados pelo administrador da plataforma;

Aplicações Federadas, onde a estratégia de acesso autentica o dispositivo para cada aplicação nesta condição de uso;

Baseado em modo Proxy: similar ao modo de operação de lista permitida (endereços IP), onde o administrador pode configurar e associar o acesso a um website hospedado.

Quantidade: 70 unidades

1.3.6 - ITEM 6 - TREINAMENTO PARA A SOLUÇÃO FIREWALL

A solução também deverá contemplar os serviços de instalação, configuração e treinamento dos técnicos da prefeitura de Hortolândia. Deverá abranger também o treinamento no formato hands-on no próprio da prefeitura municipal de Hortolândia. O treinamento deverá ser ministrado por profissionais treinados e certificados pelo fabricante da solução ofertada;

Para a empresa vencedora do certame, os profissionais responsáveis pelo treinamento deverão obrigatoriamente ser detentores de certificação válida e reconhecida, emitida pelo fabricante das soluções fornecidas, cuja comprovação se dará mediante a apresentação dos respectivos certificados com antecedência mínima de cinco dias úteis em relação à data de início do treinamento, sob pena de descumprimento das exigências contratuais.

Após treinamento os profissionais da prefeitura municipal de Hortolândia deverão receber certificados de treinamento com a quantidade de horas realizadas de curso;

Fornecer treinamento abrangente para a equipe de TI da prefeitura municipal de Hortolândia sobre o gerenciamento e operação da solução.

O treinamento deverá ser de no mínimo 16 horas e contemplar até doze participantes;

Para o escopo do treinamento, serão aceitos as atividades abaixo como mínimo possível de conteúdo nos treinamentos:

Nivelamento dos alunos, Validação de conhecimento, Zonas e Regras

1.3.6.1 - Itens do Treinamento Básico:

- ✓ NAT;
- ✓ VPN - Site/Site;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

- ✓ VPN - Client/Site;
- ✓ Content Filter;
- ✓ Integração LDAP;
- ✓ Controle por grupos;
- ✓ Intrusion Prevention;
- ✓ Gateway AV;
- ✓ Gateway Anti Spyware;
- ✓ Load Balancing;
- ✓ Roteamento Estático;
- ✓ Roteamento Dinâmico

1.3.6.2 - Itens do Treinamento Avançado:

- ✓ VPN - Tunnel Interface;
 - ✓ App Control;
 - ✓ App Rules;
 - ✓ Restrição de Banda / Controle Banda - BWM;
 - ✓ Restrição de Apps;
 - ✓ Melhores práticas;
 - ✓ Administração Solução para acesso seguro à aplicação privada e ZTNA;
- Metodologia de resolução de problemas;

1.3.6.3 - Boas Práticas:

- ✓ Como achar o problema;
- ✓ Encerramento;
- ✓ Exemplos do dia a dia;
- ✓ Tira dúvidas;

Quantidade: 01 unidade.

2 - JUSTIFICATIVA:

2.1 - Reconhecendo a crescente importância da segurança da informação no contexto atual, a prefeitura de Hortolândia busca fortalecer seus mecanismos de proteção, garantindo a integridade, confidencialidade e disponibilidade de seus sistemas e dados.

Tendo em vista que a prefeitura é constantemente alvo de ataques cibernéticos e que nos últimos meses tivemos uma invasão que quase colocou a prefeitura em paralisação por tempo indeterminado, precisamos com urgência adquirir uma solução que nos garanta segurança em conexões remotas e acessos de internet com garantia e segurança. A solução ainda vai garantir a possibilidade de redundância de conexão de internet em locais externos ao paço municipal que tenham a necessidade de conexão redundante para que os trabalhos não parem com o rompimento de cabeamento



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

de fibra óptica.

Diante do cenário de ameaças cibernéticas em constante evolução, imprescindível que a administração pública adote medidas robustas para salvaguardar suas informações sensíveis e garantir o adequado funcionamento de suas operações. Nesse sentido, a aquisição de uma solução de firewall moderna e eficiente é essencial para minimizar riscos, prevenir incidentes de segurança e assegurar a continuidade das atividades institucionais.

O firewall desempenha um papel crucial na proteção dos ativos digitais da prefeitura de Hortolândia, atuando como uma barreira de defesa que controla o fluxo de dados entre redes, monitorando e filtrando o tráfego com base em regras predefinidas. Essa solução tecnológica oferece uma camada adicional de proteção, permitindo o estabelecimento de políticas de segurança rigorosas, a identificação de atividades suspeitas e a prevenção de acessos não autorizados.

A escolha adequada de uma solução de firewall é fundamental para garantir que a prefeitura de Hortolândia esteja alinhada as melhores práticas de segurança da informação, bem como as normas e regulamentares vigentes.

Ao adotar uma abordagem abrangente e proativa, a prefeitura reafirma seu compromisso em proteger os dados e a privacidade dos cidadãos, promovendo a confiança e a transparência em suas operações.

Portanto, este Termo de Referência estabelece os critérios técnicos e operacionais necessários para a seleção de uma solução de firewall que atenda aos requisitos específicos da prefeitura de Hortolândia. Busca-se, assim, estabelecer um ambiente seguro e resiliente, capaz de enfrentar as ameaças em constante evolução e garantir a continuidade dos serviços prestados.

3 - COTA AMPLA / RESERVADA

A presente licitação será de livre concorrência sem reserva de cota para microempresas e empresa de pequeno porte, devido a especificidade do objeto. O objeto tratado nesse TR é fornecido por empresas de grande porte. Outra observação que precisa ser considerada é que a divisão de cota poderia, ao final do processo licitatório, resultar em várias empresas participando dos mesmos serviços e isso poderia causar um prejuízo técnico além de dificultar a fiscalização e a obtenção de melhor qualidade na prestação dos serviços.

4 - DOS PRAZOS, ENTREGA, INSTALAÇÃO E RECEBIMENTO DOS PRODUTOS

O prazo da Ata de Registro de Preços será de 12 (doze) meses, contados da assinatura.

A Ata de Registro de Preços poderá ser prorrogada nos termos da Lei Federal nº 14.133/2021.

O prazo de entrega será de até 60(sessenta) dias, contados da emissão da Autorização de Fornecimento.

O prazo das licenças será de 60(sessenta) meses.

4.1 - Entrega da solução:

- ✓ A proposta deverá prever a instalação física e configuração de cada produto suportado de acordo com as necessidades do ambiente específico da Prefeitura do Município de Hortolândia, para assegurar que o dispositivo esteja pronto para a implementação no ambiente de rede IP da prefeitura;
- ✓ Atualizações de firmware para versão(ões) recomendada(s) pelo fornecedor, conforme necessário;
- ✓ Assistência para definir os requisitos do caso de uso da prefeitura;



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

- ✓ Configuração dos recursos e funcionalidades do produto para atender ao caso de uso da prefeitura;
- ✓ Validação da funcionalidade de cada Produto suportado;
- ✓ Na conclusão deste Serviço, a empresa vencedora deverá conduzir uma breve sessão de orientação sobre o Produto suportado e fornecerá a documentação da implementação;

4.2 - Instalação da solução:

Este serviço fornece a instalação e implementação de dois dispositivo de segurança de rede firewall Tipo 1, cinco do tipo 2 e cinco do tipo 3 de forma conjunta com a equipe técnica da prefeitura em treinamento para conhecimento e aprendizagem. Os demais serão configurados pela equipe técnica da prefeitura e em caso de dúvidas e dificuldades a empresa vencedora disponibilizará canais de comunicação para que as dúvidas e necessidades de configuração sejam sanadas com um prazo máximo de 24 horas.

4.2.1 - Este Serviço inclui:

Instalação física e configuração de cada roduto suportado de acordo com as necessidades do ambiente específico da prefeitura de Hortolândia, para assegurar que o dispositivo esteja pronto para a implementação no ambiente de rede IP da prefeitura de Hortolândia;

Atualizações de firmware para versão(ões) recomendada(s) pelo fornecedor, conforme necessário; Assistência para definir os requisitos do caso de uso da prefeitura de Hortolândia;

Configuração dos recursos e funcionalidades do produto para atender ao caso de uso da prefeitura de Hortolândia;

Validação da funcionalidade de cada Produto suportado;

Na conclusão deste Serviço, a empresa vencedora deverá conduzir uma breve sessão de orientação sobre o produto suportado e fornecerá a documentação da implementação.

4.2.2 - As principais etapas da implantação da solução:

Confirmar a execução da atividade e as datas de instalação;

Destacar as dependências cruciais da atividade, do local de instalação no ambiente da prefeitura municipal de Hortolândia e das datas de envio do produto e de instalação que serão planejados junto ao departamento de infraestrutura de TI.;

Assegurar que a prefeitura municipal de Hortolândia por seu departamento de infraestrutura de TI analise, aceite e cumpra os termos e as condições deste Serviço.

4.2.3 - Planejamento da solução:

A prefeitura municipal de Hortolândia deve fornecer os requisitos técnicos para instalação conforme modelo de equipamento;

A prefeitura municipal de Hortolândia deverá fornecer à empresa vencedora os detalhes sobre a arquitetura de rede existente;

A empresa vencedora deve criar um plano de implementação do Serviço válido com base na configuração do



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

hardware e software da prefeitura de Hortolândia.

4.2.4 - Implementação e teste:

Instalação do dispositivo de segurança de rede (não se aplica à instalação remota): Retirar da embalagem e verificar todo o hardware antes da instalação;

Verificar se a prefeitura municipal de Hortolândia possui tomadas adequadas e espaço físico suficiente para a instalação;

Para instalação em rack a) Montar o(s) dispositivo(s) no rack; b) Instalar e posicionar todos os cabos de alimentação fornecidos junto com o equipamento de Firewall.

Ligar o(s) dispositivo(s) usando o(s) cabo(s) de interconexão fornecido(s) pela empresa vencedora e conectar o dispositivo à rede;

Verificar se há conectividade de link na rede da prefeitura municipal de Hortolândia; Registre-se e ativar o(s) dispositivo(s) e as chaves de licença complementares (se aplicável); Definir as configurações de sistema e recursos de administração;

Configurar o modo de operação, zonas e interfaces de rede; Incluir até

4 interfaces para dispositivos de firewall tipos 2 e 3; Incluir até 24

interfaces para dispositivos de firewall tipo 1;

Configurar o failover / failback da WAN e balanceamento de cargas (se aplicável); Incluir até

4 interfaces para dispositivos de firewall tipo 2 e 3;

Incluir até 24 interfaces para dispositivos de firewall do tipo 1; Configurar endereço e objetos serviços;

Incluir até 50 objetos para dispositivos de firewall tipo 2 e 3; Incluir

até 500 objetos para dispositivos de firewall tipo 1; Configurar a

conversão de endereços de rede (NAT);

Incluir até 25 políticas para dispositivos de firewall tipo 2 e 3; Incluir

até 100 políticas para dispositivos de firewall do tipo 1;

Configurar políticas de firewall, incluindo a proteção contra inundação e gerenciamento de banda; Incluir até

50 políticas para dispositivos de firewall do tipo 2 e 3;

Incluir até 150 políticas para dispositivos de firewall do tipo 1; Configurar

as regras de aplicação e visualização de painel; Configurar o IPSec VPN:

site-site e cliente-site;

Inclui até 10 VPNs para dispositivos de firewall tipo 2 e 3; Incluir até

50 VPNs para dispositivos de firewall tipo 1;

Configurar a DPI (inspeção profunda de pacotes) do tráfego criptografado SSL; Configurar a

zona sem fio e até 2 pontos de acesso virtuais;

Configurar os recursos de segurança sem fio e serviços de convidado sem fio (observação: isto não inclui a configuração sem fio nos dispositivos da prefeitura municipal de Hortolândia);

Configurar a autenticação a nível de usuário usando contas locais ou os servidores de autenticação fornecidos



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

pelo prefeitura municipal de Hortolândia; Configurar e ajustar a Alta Disponibilidade;

Criar serviços de segurança (aplica-se apenas a anti-vírus, anti-spyware, prevenção de intrusões e filtros de conteúdo do gateway);

Demonstrar ao cliente a interface web e recursos opcionais do equipamento de firewall.

4.2.5 - Familiarização com o produto:

A empresa vencedora deverá realizar uma breve sessão de orientação e analisar com o prefeitura de Hortolândia a documentação associada;

Essa visão geral não substitui nenhum curso de treinamento que a empresa vencedora terá que realizar junto aos funcionários do departamento de infraestrutura de TI para os produtos ofertados;

Fornecer a documentação a prefeitura municipal de Hortolândia, especificando os Serviços executados.

4.2.6 - Incrementação e Implantação:

Fornecer um plano de implementação detalhado, incluindo cronogramas, marcos e requisitos de recursos.

Realizar uma avaliação completa do nosso ambiente existente e fornecer recomendações para a implantação ideal.

4.3 - Encerramento do projeto:

Remover todo o material da embalagem para uma área designada pela prefeitura nas imediações do local da instalação (a uma distância de no máximo 10 metros do local da instalação) ou combinar com o departamento de infraestrutura de TI para que a remoção seja feita por ele;

Fornecer URL a prefeitura de Hortolândia para acesso de documentação do produto, guia de solução e notas de lançamento;

Revisar as notas de lançamento com a prefeitura de Hortolândia, sempre que necessário; Obter a confirmação da prefeitura municipal de Hortolândia quanto aos Serviços realizados.

4.4 - Responsabilidades específicas da prefeitura municipal de Hortolândia em relação ao Serviço:

Verificar se as tomadas de energia estão corretas e se há espaço físico suficiente para a instalação; Certificar-se de que um circuito elétrico derivado com as seguintes características esteja disponível:

A tensão e a frequência exigidas, conforme indicado no manual de referência do hardware; Proteção por um disjuntor, de acordo com os códigos elétricos locais;

Circuito de alimentação, fusível de linha e comprimento de fiação em conformidade com a classificação elétrica do comutador;

Tomada aterrada compatível com o cabo de alimentação e instalada por um eletricista licenciado; Criar uma conta no site do fabricante da solução de firewall e registrar o(s) dispositivo(s) de firewall; Certificar com relação à configuração do equipamento de rede existente que:

Os endereços IP são fornecidos para serem atribuídos ao(s) dispositivo(s), conforme necessário, com antecedência;

O ambiente do Cliente é estável e funcional para que a empresa vencedora possa iniciar os serviços



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

especificados neste documento;

Fornecer a confirmação de que os Serviços foram prestados;

4.5 - Suporte técnico e garantia.

Para uma melhor familiarização a solução implementada, a empresa vencedora deve prover um pacote de 40 horas válido por 12 meses, para suporte remoto especializado nível 3, com atendimento por especialistas bilingue, baseados no Brasil.

Este suporte visa dirimir dúvidas, fazer um primeiro atendimento em caso de ocorrências e fazer a interface com os especialistas do fabricante.

Entende-se por “Suporte” ou “Manutenção”, doravante denominada unicamente como “Suporte”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de garantia. A mesma possui suas causas em falhas e erros no Software/Hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos mesmos. Este “Suporte” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

Do hardware: apoio no processo de desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação, atualização da versão de drivers e firmware, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

Do software: atualização da versão de software (firmware e qualquer outro componente necessário para o funcionamento da solução), correção de defeitos de desenvolvimento do software, de acordo com os manuais e as formas técnicas específicas do fabricante para os recursos utilizados;

Quanto às atualizações pertinentes aos softwares: Entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia do contrato.

O fabricante deverá fornecer Suporte técnico 24x7 com tempos de resposta definidos.

Abertura de chamados deverá ser diretamente no FABRICANTE via telefone (0800) ou Internet (Portal, Chat ou Sistema de Tickets) com envio de confirmação do número do chamado e demais andamentos via e-mail.

Os serviços de “Suporte” incluem:

Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas e fabricação e desenvolvimento;

Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;

Substituição de hardware por outro de igual ou superior sem perdas de desempenho e/ou comprometimento dos serviços configurados (ex: RMA).

Atualizações de software e firmware.

Serviços de inteligência de ameaças e segurança.

Opções de serviços gerenciados e consultoria especializada.

Os prazos para a prestação dos serviços devem garantir a observância ao atendimento do seguinte Acordo de Níveis



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

de Serviços (ANS) e sua SEVERIDADE.

PARA O FIREWALL TIPO 1:

SEVERIDADE CRÍTICA – Solução totalmente inoperante (Interrupção total do serviço, falha completa do firewall). Isso em caso da parada dos dois equipamentos simultaneamente (sendo problemas de hardware e/ou software):

Prazo máximo de início de atendimento remoto de até 1 hora contados a partir do horário de abertura do chamado; Em caso de não solução do problema em até 4 horas, a detentora deverá fornecer uma solução de contingência com equipamento similar e/ou superior totalmente configurado e operacional em até 24 (vinte e quatro) horas contadas a partir da abertura do chamado.

SEVERIDADE IMPORTANTE – Solução parcialmente inoperante (1 dos hardwares param de funcionar) Prazo máximo de início de atendimento remoto de até 02 horas úteis contadas a partir do horário de abertura do chamado. Em caso de identificação de problemas com hardware, deverá ser aberto a RMA em um prazo de até 72 horas do início da abertura do chamado.

SEVERIDADE ALTA - Degradação severa do desempenho, funções principais afetadas. Prazo máximo de início de atendimento remoto de até 02 horas contadas a partir do horário de abertura do chamado.

Em caso de identificação de problemas com hardware, deverá ser aberto a RMA em um prazo de até 72 horas do início da abertura do chamado.

SEVERIDADE MÉDIA – Problemas menores, sem impacto direto na operação.

Prazo máximo de início de atendimento de até 08 horas contadas a partir do horário de abertura do chamado.

SEVERIDADE BAIXA - Dúvidas, informações sobre procedimentos, Base de conhecimento sobre configuração ou atualização. Prazo máximo de início de atendimento de até 48 horas contadas a partir do horário de abertura do chamado.

SEVERIDADE EXTERNO – Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não fornecido pela detentora. Neste caso, ficam suspensos todos os prazos de atendimento até que a contratante resolva os problemas externos que provocam a inoperância da solução. Após a contratante disponibilizar o ambiente de forma estável para a reativação da solução, a detentora realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.

RMA CRÍTICA (Em caso de Severidade CRÍTICA). - O fornecedor deverá no prazo de no máximo 24 horas, habilitar uma solução de contingência para restabelecer o ambiente/serviços e no prazo máximo de 30 (trinta) dias corridos, substituir pela solução temporária pela solução definitiva.

RMA PADRÃO (Em caso de Severidade IMPORTANTE, ALTA, MÉDIA E BAIXA) - O prazo máximo para substituição do equipamento não poderá exceder 30 (trinta) dias corridos da abertura do chamado.

Um chamado técnico somente poderá ser fechado após a confirmação do responsável da contratante e o término de



PREFEITURA DO MUNICIPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado, ou se não houver resposta da contratante pelo período de 72 horas úteis, poderá ocorrer o auto encerramento.

Na abertura de chamados técnicos, serão fornecidas informações, como Número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e severidade do chamado.

A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;

A detentora poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

A detentora deve prover, após a solução implementada, um pacote de, no mínimo, 16 horas mensais durante o período de vigência do contrato, para suporte remoto especializado, com atendimento por especialistas bilíngues (português / inglês), baseados no Brasil. Este suporte visa sanar dúvidas, fazer um primeiro atendimento de nível 1 ou 2 e 3, e em caso de ocorrências e fazer a interface com os especialistas do fabricante quando necessário.

PARA O FIREWALL TIPO 2 E 3:

Para os firewall tipo 1 e 2, em caso de Severidade IMPORTANTE, ALTA, MÉDIA E BAIXA) - O prazo máximo para substituição do equipamento em troca avançada, não poderá exceder 05 (dias úteis) dias corridos da abertura do chamado.

5 – DA DOTAÇÃO ORÇAMENTÁRIA:

As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Programa deste exercício, nas dotações abaixo discriminadas:

Natureza da Despesa: Serviços de Tecnologia da Informação e Comunicação - PJ Ficha

34 - 01.02.04.131.0201.2.008.339040.01.1100000 - Secretaria de Governo Ficha 81-

02.02.04.126.0219.2.015.449040.01.1100000 - SMPUGE

Ficha 99 - 03.01.03.092.0204.2.017.339040.01.1100000 - Secretaria de Assuntos Jurídicos Ficha

148 - 05.01.04.122.0216.2.020.339040.01.1100000 - Secretaria de Administração Ficha 187 -

06.01.18.541.0223.2.033.339040.01.1100000 - Secretaria de Meio Ambiente Ficha 232 -

07.02.06.181.0224.2.041.339040.01.1000074 - Secretaria de Segurança

Ficha 250 - 08.01.22.661.0225.2.043.339040.01.1100000 - Secretaria de desenv. economico Ficha 271

- 09.01.15.452.0220.2.046.339040.01.1100000 - Secretaria de Serviços Urbanos Ficha 296 -

10.01.15.452.0226.2.051.339040.01.1100000 - Secretaria de Mobilidade Urbana Ficha 323 -

11.01.16.482.0227.2.055.339040.01.1100000 - Secretaria de Habitação

Ficha 348 - 12.01.08.244.0207.2.058.339040.01.5100000 - Secretaria de Inclusão Social Ficha

423 - 13.01.12.122.0209.2.074.339040.01.2200000 - Secretaria de Educação Ficha 564 -

14.01.15.451.0230.2.103.339040.01.1100000 - Secretaria de Obras

Ficha 599 - 15.01.10.122.0212.2.104.339040.01.3100000 - Secretaria de Saúde Ficha 725 -

16.01.13.392.0228.2.131.339040.01.1100000 - Secretaria de Cultura Ficha 762 -



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

17.01.27.812.0229.2.136.339040.01.1100000 - Secretaria de Esportes

6 – CONDIÇÕES DE PAGAMENTO:

A detentora, quando do cumprimento às Autorizações de Fornecimento, emitirá as respectivas notas fiscais/faturas, discriminando os serviços prestados.

Após a efetiva entrega e conferência dos itens, o (s) profissional (is) responsável (is) promoverá (ão) o ateste na (s) nota (s) fiscal (is), encaminhando-as para pagamento.

Os pagamentos deverão ser efetuados em 10 (dez) dias, fora a dezena, da data do ateste das notas fiscais/faturas. As notas fiscais/fatura deverão ser emitidas para o **MUNICÍPIO DE HORTOLÂNDIA** sob o número de **CNPJ 67.995.027/0001-32**, exceto quando a secretaria requisitante for a **SAÚDE**, sendo que neste caso, as notas fiscais/fatura deverão ser emitidas para o **FUNDO MUNICIPAL DE SAÚDE** sob o número de **CNPJ 13.843.145/0001-04**.

7 – CRITÉRIO DE JULGAMENTO:

Menor preço global

8 – DOCUMENTAÇÃO TÉCNICA:

8.1 - A licitante vencedora deverá apresentar comprovação de aptidão (capacitação técnico-operacional) para o item 1 – Firewall tipo 1, através de atestado de capacidade técnica emitido por pessoas jurídicas de direito privado ou público, demonstrando que a empresa licitante tenha executado serviços similares com o objeto da licitação, em qualquer quantidade. A comprovação técnica será necessária apenas para o item 1.

8.1.1 – A comprovação de capacidade técnica visa:

- ✓ Assegurar que a empresa licitante detenha conhecimento técnico e experiência prática na implantação e suporte de soluções de firewall de complexidade equivalente à demandada;
- ✓ Mitigar riscos de falhas operacionais decorrentes da inexperiência do fornecedor;
- ✓ Garantir a qualidade, a segurança e a continuidade dos serviços prestados à Administração Pública;
- ✓ Assegurar o cumprimento das especificações técnicas, de forma a garantir a efetividade da solução contratada.

A exigência referente a capacidade técnica é importante, pois, em caso de vencimento de uma empresa sem experiência na área de segurança digital, muitas das experiências de mercado não serão aplicadas nas configurações de equipamentos e softwares, podendo assim deixar brechas de segurança mesmo com a aquisição de equipamentos e softwares que foram desenvolvidos para tal objetivo.

Esse mercado é muito dinâmico e vírus e ameaças surgem todo dia, se a empresa vencedora não tiver experiência no mercado, ela poderá não atender as necessidades da administração pública e teremos gastado dinheiro sem conseguir os objetivos. Não exigir capacidade técnicas da empresa vencedora seria muito arriscado, pois, a empresa através de seus colaboradores, serão responsáveis pelo treinamento dos funcionários públicos para a perfeita utilização da solução, caso



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

a empresa não tenha esses conhecimentos adquiridos através de experiências de mercado, todo o projeto ficará comprometido.

9 – VISITA TÉCNICA

Como condição de participação, as licitantes interessadas deverão vistoriar o prédio da Prefeitura do Município de Hortolândia (Paço Municipal de Hortolândia - Palácio dos Migrantes), situado à Rua Professora Celina Franceschini Bueno, número 100 - Jardim Metropolitano - **CEP:** 13184-792 - **Bairro:** Jardim Metropolitano - Hortolândia – SP, para conhecimento das condições reais de implantação, integração e funcionamento da solução de segurança de rede de dados (Firewall) no ambiente tecnológico da Prefeitura do Município de Hortolândia.

A visita técnica deverá ser marcada previamente pela licitante, através do telefone(19)3965-1400 ramal 9028, ou email leoniciooliveira@hortolandia.sp.gov.br, com o Sr. Leonício Ornelas de Oliveira,

A visita técnica será de segunda a sexta-feira no período das 08h30min às 11h30min e das 13h30min às 16h30min, até o dia anterior ao da sessão licitatória.

O comprovante de visita técnica deverá ser apresentado pela empresa licitante junto com a documentação de habilitação, devidamente assinado e pelo servidor responsável do departamento de T.I, sob pena de inabilitação.

A não apresentação da declaração de visita técnica ensejará a inabilitação da LICITANTE.

Na visita técnica as empresas que participarão da licitação deverão verificar as conexões existentes nos equipamentos que gerenciam a rede da prefeitura para que não ocorram divergências nas propostas em relação ao tipo e velocidades das conexões bem como ao fornecimento dos cabos necessários para tais conexões.

A exigência de visita técnica fundamenta-se na necessidade de assegurar que as empresas licitantes conheçam, previamente, as condições reais de implantação, integração e funcionamento da solução de segurança de rede de dados (Firewall) no ambiente tecnológico da Prefeitura Municipal de Hortolândia. Tal medida garante que as propostas apresentadas sejam tecnicamente adequadas, precisas e plenamente exequíveis, mitigando riscos de incompatibilidades, subdimensionamentos, falhas de planejamento ou necessidade de aditivos futuros.

Fundamentação Técnica

A solução de Firewall a ser contratada envolve integração com infraestrutura existente, incluindo, mas não se limitando a:

- ✓ topologia atual da rede;
- ✓ enlaces e rotas críticos;
- ✓ arquitetura de redundância (HA);
- ✓ sistemas legados e appliances já instalados;
- ✓ políticas de segurança vigentes;
- ✓ requisitos de conectividade com data center e redes externas;
- ✓ condições físicas e lógicas para instalação dos equipamentos.

A complexidade da infraestrutura demanda que o licitante tenha conhecimento prévio do ambiente, para avaliar:

- ✓ compatibilidade da solução ofertada com as interfaces presentes;
- ✓ capacidade de processamento e throughput requerido;



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

- ✓ necessidades de módulos adicionais, licenças, blades ou serviços específicos;
- ✓ condições de energia, climatização e espaço físico no rack;
- ✓ riscos operacionais e cenários de contingência.
- ✓

Sem tal conhecimento prévio, a proposta técnica poderia apresentar falhas, como:

- ✓ oferta de equipamentos incompatíveis com o ambiente;
- ✓ dimensionamento incorreto do throughput ou sessões simultâneas;
- ✓ subestimação de serviços de integração e migração;
- ✓ ausência de componentes essenciais à operação;
- ✓ cronogramas inexequíveis.

A visita técnica assegura a aderência plena da solução e evita a necessidade de ajustes posteriores que possam gerar atrasos ou custos adicionais.

A visita, previamente agendada, não limita a competição, apenas assegura que todos tenham condições equivalentes de conhecimento do ambiente.

Objetivos da Exigência

A visita técnica permitirá:

- ✓ obtenção de informações reais sobre a infraestrutura;
- ✓ elaboração de solução tecnicamente compatível;
- ✓ redução de riscos na instalação e integração;
- ✓ definição precisa dos serviços de implantação e migração;
- ✓ melhoria da qualidade das propostas técnicas e financeiras;
- ✓ prevenção de litígios, glosas e aditivos contratuais;
- ✓ continuidade operacional da rede e dos serviços públicos críticos.

Condições para Realização da Visita Técnica

A visita será:

- ✓ agendada previamente com a Administração Municipal;
- ✓ acompanhada por servidor designado;
- ✓ registrada por meio de Declaração de Visita Técnica emitida pelo órgão;
- ✓ não será impeditiva para empresas que deleguem a visita a representante legal ou técnico munido de autorização formal.

Não serão fornecidas informações sigilosas, apenas dados essenciais para o dimensionamento adequado da solução.

Diante da complexidade inerente à implantação de uma solução de segurança de rede de dados (Firewall), a visita técnica é medida essencial, proporcional e legalmente amparada, visando garantir que as propostas apresentadas pelos licitantes reflitam conhecimento adequado do ambiente e assegurem a contratação da solução mais vantajosa para a Administração.

A licitante poderá substituir a Visita Técnica por declaração formal assinada pelo responsável técnico da licitante acerca



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA
Secretaria de Planejamento Urbano e Gestão Estratégica
Departamento de Infraestrutura da Tecnologia da Informação

do conhecimento pleno das condições e peculiaridades da contratação.

MODELO DE DECLARAÇÃO DE VISITA TÉCNICA

Declaro para os devidos fins de instrução do processo licitatório PMH - ____/2025 , Pregão ____/2025, que a Empresa _____ CNPJ _____, aqui representado por _____ CPF _____ compareceu no dia ____/____/2025 à Prefeitura do Município de Hortolândia para visita técnica, onde lhe foram apresentadas todas as informações e condições para o completo e adequado cumprimento das obrigações decorrentes desta licitação.

Responsável pela VisITA Técnica

MODELO DE DECLARAÇÃO FORMAL DE SUBSTITUIÇÃO DA VISTORIA TÉCNICA

Razão Social da Empresa], pessoa jurídica de direito privado, inscrita **no CNPJ sob o nº** [informar], com sede à [endereço completo], neste ato representada por seu representante legal, [nome completo], portador(a) do **CPF nº** [informar] e **RG nº** [informar], para fins de participação no Processo Licitatório promovido pela Prefeitura do Município de Hortolândia, cujo objeto é a Ata de registro de preços para aquisição de solução de segurança de dados – Firewall conforme Termo de Referência, vem, respeitosamente, declarar que:

- 1 - Substitui a realização de vistoria técnica presencial, em conformidade com o disposto no Edital e seus anexos, apresentando a presente declaração como instrumento comprobatório de ciência e concordância com todas as condições técnicas e operacionais relacionadas ao objeto da contratação.
- 2 - Declara ter pleno, integral e inequívoco conhecimento de todas as informações constantes do Edital e do Termo de Referência, bem como das particularidades, requisitos de infraestrutura, ambiente tecnológico, restrições, interfaces, rotinas operacionais e demais elementos indispensáveis à execução adequada do objeto licitado.
- 3 - Possui conhecimento suficiente para a elaboração da proposta, responsabilizando-se integralmente por eventuais dificuldades decorrentes do desconhecimento ou da interpretação inadequada das condições reais relacionadas à instalação, configuração e funcionamento da solução de segurança de dados (Firewall).
- 4 - Compromete-se a cumprir fielmente todas as obrigações estabelecidas no Edital, no Termo de Referência e nos demais documentos que compõem o processo licitatório, não podendo, em nenhuma hipótese, alegar desconhecimento das condições do ambiente ou das exigências técnicas do objeto contratado.

Por ser expressão da verdade, a presente declaração é firmada para todos os fins legais.

Cidade, data.

Nome do(a) Representante Legal]



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

Cargo – Razão Social da Empresa

CNPJ: informar

10 – APRESENTAÇÃO DE AMOSTRA

A licitante vencedora deverá apresentar documentos comprobatórios, por meio de relatórios ou catálogos, testes de bancada ou demo. Esses relatórios ou catálogos deverão ser apresentados de forma clara e objetiva, demonstrando a conformidade com os requisitos estabelecidos neste termo de referência.

A exigência de que a licitante vencedora apresente documentos comprobatórios — tais como relatórios técnicos, catálogos oficiais do fabricante, testes de bancada (benchmarks) ou demonstrações (demo) — visa assegurar a verificação objetiva da conformidade da solução ofertada em relação aos requisitos técnicos definidos neste Termo de Referência.

Tal medida fundamenta-se na necessidade de garantir que a solução de segurança de rede (firewall) atenda integralmente às especificações mínimas de desempenho, compatibilidade, funcionalidades e requisitos de segurança estabelecidos pela Administração Pública, evitando riscos operacionais, prejuízos ao erário ou aquisições inadequadas.

Soluções de segurança de rede (firewall de próxima geração, IDS/IPS, antivírus de tráfego, filtragem inteligente, inspeção SSL etc.) envolvem:

- ✓ recursos de alto desempenho;
- ✓ funcionalidades críticas para proteção de dados e continuidade dos serviços públicos;
- ✓ configurações avançadas que variam entre fabricantes;
- ✓ impacto direto na disponibilidade e segurança da infraestrutura de TI.

Diante disso, a simples apresentação de propostas comerciais não é suficiente para comprovar que o equipamento ofertado realmente entrega:

- ✓ a capacidade de processamento exigida;
- ✓ o throughput real em ambiente com inspeção completa;
- ✓ as funcionalidades de segurança (NGFW, VPN, IDPS, Web Filter, Antimalware etc.);
- ✓ integração com a arquitetura atual da instituição;
- ✓ conformidade com protocolos, padrões e requisitos técnicos mínimos.

Relatórios técnicos, catálogos oficiais, testes de bancada ou demonstrações práticas possibilitam a comprovação objetiva e verificável da conformidade da solução, reduzindo riscos de aquisição inadequada.

A exigência dos documentos comprobatórios:

- ✓ Evita o fornecimento de produtos subdimensionados ou que não atendam aos requisitos reais.
- ✓ Reduz riscos de incompatibilidade com a infraestrutura existente.



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

- ✓ Assegura transparência e isonomia, pois todos os licitantes devem comprovar as mesmas condições de aderência.
- ✓ Promove aquisição mais vantajosa, pois permite validar desempenho e funcionalidades antes do recebimento definitivo.
- ✓ Favorece maior segurança jurídica, por registrar evidências objetivas de que a solução atende integralmente ao Termo de Referência.

Assim, convidamos as empresas interessadas e qualificadas a apresentarem suas propostas de solução de firewall, de acordo com os critérios estabelecidos neste termo de referência, a fim de que possamos fortalecer a segurança da Prefeitura do Município de Hortolândia e garantir proteção efetiva de nossos ativos digitais."

A contratação será na modalidade de ata de registro de preços, possibilitando assim, o crescimento do sistema de segurança com a participação das secretarias da prefeitura de forma distribuída. Essa distribuição poderá ser realizada também na questão dos acessos remotos, onde cada secretaria poderá adquirir as licenças necessárias para que seus servidores possam realizar trabalhos de forma remota quando necessário.

11 – PROVA DE CONCEITO

Não se aplica

12 – CONSÓRCIO

Considerando a natureza crítica do objeto, optamos pela **vedação à participação de empresas reunidas em consórcio** na presente licitação, pelos motivos técnicos e operacionais a seguir expostos.

Complexidade e Sensibilidade da Solução

A solução de firewall a ser adquirida constitui elemento essencial para a proteção da rede corporativa, realizando inspeção de tráfego, prevenção de ataques, controle de acesso e mitigação de ameaças avançadas.

A execução adequada desses serviços exige **coerência operacional e integração completa entre hardware, software e suporte técnico**, o que demanda responsabilidade técnica centralizada.

Necessidade de Responsabilidade Única

A implantação e o suporte do firewall requerem **responsabilidade técnica única**, especialmente para resposta a incidentes, aplicação de patches, atualização de assinaturas de ameaças e gestão de políticas de segurança.

A participação de empresas consorciadas poderia fragilizar essa responsabilidade, dificultando a definição de accountability em falhas, a comunicação técnica e a continuidade operacional.

Garantia de Suporte e Manutenção Especializada

A solução exige:

- ✓ suporte técnico especializado 24x7,
- ✓ atendimento a SLAs rígidos,



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

- ✓ atualização contínua das bases de inteligência de ameaças.

O fracionamento de atividades entre consorciadas pode prejudicar o cumprimento desses requisitos e comprometer a efetividade do suporte, além de dificultar a aplicação de penalidades e o monitoramento da execução contratual.

Integração com a Infraestrutura Existente

A solução deverá ser diretamente integrada aos ativos de rede, servidores, sistemas de autenticação e demais componentes críticos existentes na Administração. Essa integração requer homogeneidade de procedimentos e atuação coordenada, condições que são prejudicadas em estruturas consorciadas, elevando o risco de incompatibilidades e atrasos na implantação.

Riscos para a Segurança da Informação

A segurança cibernética depende de processos contínuos, padronizados e integrados. A fragmentação de responsabilidades, típica de consórcios, pode gerar lacunas operacionais e administrativas, aumentando a superfície de risco e a possibilidade de incidentes ou indisponibilidades.

Diante da necessidade de segurança, integridade, continuidade operacional e responsabilização técnica única na implantação e manutenção da solução de firewall, justifica-se a vedação à participação de empresas em consórcio na presente contratação. A medida é necessária para garantir a efetividade da solução, reduzir riscos e assegurar a adequada execução contratual.

13 – SUBCONTRATAÇÃO

Será vedada a subcontratação, cessão total ou parcial da futura aquisição pois isso poderia apresentar riscos e desvantagens, como perda de controle sobre a segurança da rede, falta de conhecimento técnico especializado, dificuldades na gestão e comunicação, e potenciais problemas de conformidade.

14 – LONGITUDE E LATITUDE DO LOCAL QUE OCORRERÁ A OBRA

Não se aplica

15 – OBRIGAÇÕES DA detentora/ DETENTORA:

A (s) empresa (s) detentora (s) deverá (ão):

- a-) Efetuar as entregas dos Itens, em estrita observância das especificações do termo de referência e seus anexos, bem como da proposta;
- b-) Apresentar nota fiscal/fatura de conforme a Autorização de Fornecimento;
- c-) Promover a correção da nota fiscal/fatura que não for aprovada, no prazo máximo 05(cinco) dias úteis; d-) Arcar com todos os custos decorrentes dos transportes, carga e descarga dos produtos até o local de entrega;
- e-) Indicar preposto com poderes para representá-la perante a Municipalidade em tudo que se relacionar com o fornecimento dos itens;
- f-) Manter, durante o período de vigência da Ata de Registro de Preços as condições de habilitação e qualificação exigidas para a participação na licitação;
- g-) Comunicar, por escrito, quando da ocorrência de anormalidades, tais como: interdição, suspensão, descontinuação



PREFEITURA DO MUNICÍPIO DE HORTOLÂNDIA

Secretaria de Planejamento Urbano e Gestão Estratégica

Departamento de Infraestrutura da Tecnologia da Informação

de qualquer item ofertado, propondo, quando for o caso, sua substituição por outro produto da mesma marca, mantidas todas as condições avençadas, mediante aceite da Administração;

h-) Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto da Ata de Registro de Preços);

i-) Comunicar, por escrito, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

j-) Fornecer canal de comunicação para suporte junto ao fabricante durante todo o prazo do contrato (60) meses para possíveis configurações e atualizações dos equipamentos e softwares ofertados neste processo.

k-) Para casos de configuração e atualização de equipamentos/software o canal de comunicação da empresa vencedora, com auxílio do fabricante, deverá atender os chamados em um prazo máximo de 24 horas;

l-) Estar ciente e concordar que a garantia dos produtos e softwares ofertados neste processo é de 60 meses. Desta forma a empresa terá que dar suporte para todos os equipamentos e softwares utilizados e

em caso de necessidade de troca dos equipamentos, a empresa deverá informar o prazo para realização do processo e o mesmo deve ser aprovado pelo departamento de infraestrutura de T.I da prefeitura.

m-) Fornecer todos os cabos e conexões necessárias para a perfeita instalação dos equipamentos no ambiente de rede da prefeitura municipal de Hortolândia. Todas as dúvidas deverão ser sanadas na visita técnica. Caso a empresa decida não realizar a visita técnica, estará ciente de que deverá fornecer todos os cabos e demais materiais necessários para as conexões do ambiente de rede da prefeitura.

16- OBRIGAÇÕES DO MUNICÍPIO DE HORTOLÂNDIA:

O Município de Hortolândia deverá:

a-) Receber provisoriamente os itens, disponibilizando local, data e horário;

b-) Verificar minuciosamente, no prazo fixado, a conformidade dos produtos recebidos provisoriamente com as especificações constantes do termo de referência e seus anexos e da proposta, para fins de aceitação e recebimentos definitivos;

c-) Acompanhar e fiscalizar o cumprimento das obrigações da (s) detentora (s), através de servidor especialmente designado;

1.1 Efetuar os pagamentos nos prazos previstos.

17 – CONSIDERAÇÕES GERAIS:

Os objetos descritos neste termo de referência não conduzem às marcas e/ou fornecedores, portanto a definição dos produtos licitados é precisa, suficiente e clara, de modo que não são definições excessivas, irrelevantes, subjetivas ou desnecessárias e não limitam a competição.

Leonicio Ornelas de Oliveira Hemerson

Hemerson Donizete Laranjeira.

Hortolândia, 29 de Setembro de 2025.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

ANEXO III

PROPOSTA FINAL

Pregão Eletrônico nº 06/2026

Data da sessão em 02/02/2026, Horário: 08h30min

Proponente: _____

Endereço: _____

Cidade: _____ **Estado:** _____

CNPJ/MF nº: _____

Telefone: _____

e-mail: _____

Objeto: Ata de registro de preços para Aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

DADOS BANCÁRIOS DA PROPONENTE

Banco:

Nome da Agência:

Número da Agência:

Número da Conta – Corrente:



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

DADOS DA(S) PESSOA(S) QUE IRÁ(AO) FIRMAR O INSTRUMENTO CONTRATUAL:

Nome:

Estado Civil:

Profissão:

R.G. nº

CPF/MF nº

Endereço:

Validade da proposta:

Valor total da proposta: R\$ ____, __ (_____)

ITEM	COD.	DESCRIÇÃO	UND	QTD	MARCA	PREÇO UNITÁRIO	PREÇO TOTAL

Representante da pessoa jurídica



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

ANEXO IV

Minuta da ATA de Registro de Preços

MUNICÍPIO DE HORTOLÂNDIA

PROCESSO ADMINISTRATIVO Nº 100876/2025

ATA Nº «ATA», RESULTANTE DO PREGÃO ELETRÔNICO Nº ____/2026, QUE FAZEM ENTRE SI O MUNICÍPIO DE HORTOLÂNDIA, POR INTERMÉDIO DO (A) «SEC_REQUISITANTE», E «**DETENTORA**».

O **MUNICÍPIO DE HORTOLÂNDIA**, pessoa jurídica de direito público interno, sediada na Rua Professora Celina Franceschini Bueno, nº 100, Bairro Jardim Metropolitano, no Município de Hortolândia – SP, cadastrada junto ao Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda (CNPJ/MF) sob nº 67.995.027/0001-32, neste ato, representado pelo(a) Secretário(a) Municipal, Sr.(a) «**Nome_Secretárioa**», «Dados_Secretário», doravante denominado **CONTRATANTE**, e, de outro lado, a empresa «**DETENTORA**», pessoa jurídica de direito privado, sediada na «END_LOGRADOURO», «N__COMPL», Bairro «BAIRRO», CEP: «CEP», no Município de «CIDADE», Estado de «ESTADO», cadastrada junto ao Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda – (CNPJ/MF) sob o nº «CNPJ», com Inscrição Estadual registrada sob nº «IE», neste ato representado por seu «CARGO_RESP_LEGAL» Sr. «**NOME_RESP_LEGAL**», «NACIONALIDADE», «ESTADO_CIVIL», «QUALIFICAÇÃO_PROFISSIONAL», portador da Cédula de Identidade (R.G.) nº «RG_C_UF_EMISSOR», devidamente inscrito junto ao Cadastro de Pessoas Físicas do Ministério da Fazenda – (CPF/MF) sob nº «CPF», doravante denominada **DETENTORA**, firmam a presente **ATA DE REGISTRO DE PREÇOS**, mediante as cláusulas e condições a seguir enunciadas:



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a Ata de registro de preços para Aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia, de acordo com as especificações contidas no Termo de referência, e nas demais condições aqui estipuladas.

1.2. Objeto da contratação:

ITEM	CÓDIGO	QTDE	UN.	DESCRIÇÃO	MARCA	VALOR UNIT	VALOR TOTAL
01	12.3.3929	02	Un	Firewall tipo 1			
02	12.3.3930	30	Un	Firewall tipo 2			
03	12.3.3931	110	Un	Firewall tipo 3			
04	12.3.3932	01	Un	Solução de Gerenciamento Centralizado e relatório NGFW Tipos 1, 2 e 3			
05	12.3.3933	70	Un	Solução para acesso seguro à aplicação privada e ZTNA			
06	12.3.3939	01	Serv.	Treinamento para a solução Firewall			

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta da **DETENTORA**;

1.3.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência desta ATA de Registro de Preços é de **12 (doze) meses**, contados da assinatura deste instrumento, podendo ser prorrogado nos termos da legislação vigente.

2.1.1. Esta ATA poderá ser assinada:

2.1.1.1. Por meio de **assinatura digital qualificada**, caso em que o termo



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

inicial da vigência corresponderá à data da assinatura deste instrumento, considerando-se, para tanto, o momento em que a última parte signatária formalizar sua assinatura eletrônica, nos termos da [Medida Provisória nº 2.200-2/2001](#) e demais normas regulamentares pertinentes; ou

2.1.1.2. Por meio de **assinatura física**, por ambas as partes, caso em que o **termo inicial da vigência** será a data constante ao final desta ATA.

2.1.2. O **termo final da vigência** dar-se-á no mesmo dia e mês do ano subsequente ao do início da vigência, ressalvada a possibilidade de prorrogação, observadas as formalidades legais e as condições ajustadas entre as partes.

2.1.3. A assinatura eletrônica, conforme regulamentação vigente, equipara-se à assinatura manuscrita para todos os efeitos legais, garantindo a validade, autenticidade e integridade deste instrumento.

2.2. Se esta ATA for prorrogada, os quantitativos **poderão** ser renovados

2.3. As prorrogações de prazo de vigência serão formalizadas mediante celebração dos respectivos termos de aditamento, respeitadas as condições prescritas na [Lei Federal nº 14.133/2021](#).

2.3.1. A não prorrogação do prazo de vigência, por conveniência desta Prefeitura não gerará a empresa **DETENTORA** direito a qualquer espécie de indenização;

2.4. A **DETENTORA** poderá se opor à prorrogação de que trata o subitem anterior, desde que o faça mediante documento escrito, recebido pela Unidade **CONTRATANTE** em até cento e vinte dias antes do vencimento desta ATA, ou de cada uma das prorrogações do prazo de vigência.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a esta ATA de Registro de Preços.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA – PREÇO

5.1. O valor total da presente ATA de Registro de Preços é de **R\$** (.....).

5.2. 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.

CLÁUSULA SEXTA – PAGAMENTO

6.1. A **DETENTORA**, quando do cumprimento das Autorizações de Fornecimento, emitirá as respectivas notas fiscais/faturas, discriminando as quantidades e produtos fornecidos.

6.2. Após a efetiva entrega e conferência dos itens, o(s) profissional(is) responsável(is) promoverá(ão) o ateste na(s) nota(s) fiscal(is), encaminhando-as para pagamento.

6.3. Os pagamentos deverão ser efetuados em 10 (dez) dias, fora a dezena, da data do ateste das notas fiscais/faturas.

6.4. As notas fiscais/fatura deverão ser emitidas para o **MUNICÍPIO DE HORTOLÂNDIA**, sob o número de **CNPJ 67.995.027/0001-32**.

6.5. Quando as Autorizações de fornecimento forem emitidas pela Secretaria Municipal de Saúde, as notas fiscais/fatura deverão ser emitidas para o **FUNDO MUNICIPAL DE SAÚDE**, sob o número de **CNPJ 13.843.145/0001-04**.

6.6. Por força da [Instrução Normativa RFB nº 2043/2021](#), para fins Tributários, os valores para recolhimento previdenciário (INSS) devem estar discriminados na Nota Fiscal;

6.7. Considerando decisão proferida pelo STF – RE 1.293.453 em 11/10/2021 e por força do [Decreto Municipal 4.947/2021](#) que trata das regras de retenção de tributos no pagamento a fornecedores por Órgãos e Entidades do Poder Executivo, dispostas na [Instrução Normativa RFB nº 1234/2012](#), ao efetuar os pagamentos o **CONTRATANTE** procederá à



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

retenção do imposto de renda (IR).

6.7.1. As retenções serão realizadas no momento do pagamento dos valores decorrentes da prestação de serviços contratados ou fornecimento dos bens contratados, uma vez atestados e liquidados, mediante recolhimento aos cofres municipais, nos termos do [inciso I do art. 158 da Constituição Federal de 1988](#);

6.7.2. As retenções serão efetuadas sobre qualquer forma de pagamento, inclusive os pagamentos antecipados por conta de fornecimento de bens ou prestação de serviços, para entrega futura;

6.7.3. Não estão sujeitos à retenção do IR na fonte os pagamentos realizados a pessoas ou serviços e mercadorias elencados no [art. 4º da Instrução Normativa RFB nº 1234, de 11 de janeiro de 2012](#).

6.8. Nos casos de eventuais atrasos de pagamento, desde que a **DETENTORA** não tenha concorrido de alguma forma, deverá ser acrescido de encargos moratórios proporcionais aos dias de atraso, apurados desde a data limite prevista para o pagamento até a data do efetivo pagamento, à taxa de 6% (seis por cento) ao ano, aplicando-se a seguinte fórmula:

$$EM = I \times N \times VP$$

EM = Encargos Moratórios a serem acrescidos ao valor originariamente devido;

I = Índice de atualização financeira, calculado segundo a fórmula:

$$I = \frac{(6 / 100)}{365}$$

N = Número de dias entre a data limite prevista para o pagamento e a data do efetivo pagamento;



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

VP = Valor da Parcela em atraso.

CLÁUSULA SÉTIMA – REAJUSTE

7.1. Os preços inicialmente contratados poderão ser reajustados na hipótese de ocorrência do [artigo 84 da Lei 14.133/2021](#).

7.1.1. A data base do orçamento estimado é 01/10/2025.

7.2. O reajuste se dará após negociação entre as partes, observando-se como limite máximo a variação do índice IPCA/IBGE.

7.3. O reajuste de preços deverá ser solicitado formalmente pela **DETENTORA**.

7.4. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o **CONTRATANTE** pagará à **DETENTORA** a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

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

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA – OBRIGAÇÕES DO CONTRATANTE

8.1. Sem prejuízo das obrigações descritas no Termo de referência, são obrigações do **CONTRATANTE**:

8.2. Exigir o cumprimento de todas as obrigações assumidas pela **DETENTORA**, de acordo com a ATA de Registro de Preços e seus anexos;



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

- 8.3.** Receber o objeto no prazo e condições estabelecidas no Termo de Referência;
- 8.4.** Notificar a **DETENTORA**, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;
- 8.5.** Acompanhar e fiscalizar a execução da ATA de Registro de Preços e o cumprimento das obrigações pela **DETENTORA**;
- 8.6.** Comunicar a empresa 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, de 2021](#);
- 8.7.** Efetuar o pagamento a **DETENTORA** do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos na presente ATA de Registro de Preços;
- 8.8.** Aplicar a **DETENTORA** as sanções previstas na lei e nesta ATA de Registro de Preços;
- 8.9.** Cientificar o órgão de representação judicial da Prefeitura Municipal de Hortolândia para adoção das medidas cabíveis quando do descumprimento de obrigações pela **DETENTORA**;
- 8.10.** Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução da presente ATA de Registro de Preços, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.
- 8.10.1.** A Administração terá o prazo de 01 (um) mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.
- 8.11.** Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela **DETENTORA** no prazo máximo de 01 (um) mês.
- 8.12.** Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

8.13. A Administração não responderá por quaisquer compromissos assumidos pela **DETENTORA** com terceiros, ainda que vinculados à execução da ATA de Registro de Preços, bem como por qualquer dano causado a terceiros em decorrência de ato da **DETENTORA**, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA – OBRIGAÇÕES DA DETENTORA

9.1. Sem prejuízo das obrigações descritas no Termo de referência, são obrigações da **DETENTORA**:

9.2. A **DETENTORA** deve cumprir todas as obrigações constantes desta ATA de Registro de Preços e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.3. Comunicar ao **CONTRATANTE**, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.4. Atender às determinações regulares emitidas pelo fiscal ou gestor da ATA de Registro de Preços ou autoridade superior ([art. 137, II, da Lei n.º 14.133, de 2021](#)) e prestar todo esclarecimento ou informação por eles solicitados;

9.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal da ATA de Registro de Preços, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução da ATA de Registro de Preços pelo **CONTRATANTE**, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

9.7. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas,



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao **CONTRATANTE** e não poderá onerar o objeto da ATA de Registro de Preços;

9.8. Comunicar ao Fiscal da ATA de Registro de Preços, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto.

9.9. Paralisar, por determinação do **CONTRATANTE**, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.10. Manter durante toda a vigência da ATA de Registro de Preços, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.11. Cumprir, durante todo o período de execução da ATA de Registro de Preços, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação ([art. 116, da Lei n.º 14.133, de 2021](#));

9.12. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal da ATA de Registro de Preços, com a indicação dos empregados que preencheram as referidas vagas ([art. 116, parágrafo único, da Lei n.º 14.133, de 2021](#));

9.13. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento da ATA de Registro de Preços;

9.14. 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, de 2021](#).

9.15. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do **CONTRATANTE**;

9.16. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

perfeito cumprimento das cláusulas desta ATA de Registro de Preços, 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;

9.17. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.

9.18. Submeter previamente, por escrito, ao **CONTRATANTE**, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

9.19. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

9.20. Observar e seguir à risca, a todas as disposições contidas no Manual de boas-vindas para prestadores de serviço, anexo a esta ATA de Registro de Preços.

CLÁUSULA DÉCIMA – LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

10.1. As partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, nos termos da Lei Geral de Proteção de Dados – LGPD ([Lei nº 13.709, de 14 de agosto de 2018](#));

10.1.1. O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos artigos [7º](#), [11](#) e/ou [14](#) da [Lei nº 13.709/2018](#) às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e informados ao titular.

10.2. A **DETENTORA** obriga-se ao dever de proteção, confidencialidade, sigilo de toda informação, dados pessoais e base de dados a que tiver acesso, nos termos da LGPD, suas alterações e regulamentações posteriores, durante o cumprimento do objeto descrito no instrumento contratual;



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

10.2.1. A **DETENTORA** não poderá se utilizar de informação, dados pessoais ou base de dados a que tenham acesso, para fins distintos da execução dos serviços especificados no instrumento contratual;

10.2.2. Em caso de necessidade de coleta de dados pessoais dos titulares mediante consentimento, indispensáveis à própria prestação do serviço, esta será realizada após prévia aprovação do município de Hortolândia, responsabilizando-se a **DETENTORA** pela obtenção e gestão.

10.3. A **DETENTORA** obriga-se a implementar medidas técnicas e administrativas aptas a promover a segurança, a proteção, a confidencialidade e o sigilo de toda informação, dados pessoais e/ou base de dados que tenha acesso, a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito; tudo isso de forma a reduzir o risco ao qual o objeto da ATA de Registro de Preços ou o município de Hortolândia está exposto;

10.4. A **DETENTORA** deverá manter os registros de tratamento de dados pessoais que realizar, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer tempo;

10.4.1. A **DETENTORA** deverá permitir a realização de auditorias do município de Hortolândia e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações relacionadas à sistemática de proteção de dados;

10.4.2. A **DETENTORA** deverá apresentar ao município de Hortolândia, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como os demais dispositivos legais aplicáveis.

10.5. A **DETENTORA** se responsabilizará por assegurar que todos os seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados, documento que deverá estar disponível em caráter permanente para exibição ao município de Hortolândia, mediante solicitação;

10.5.1. A **DETENTORA** deverá promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do município de Hortolândia, em caso de desligamento de funcionário das atividades inerentes à execução da presente ATA de Registro de Preços.

10.6. A **DETENTORA** não poderá disponibilizar ou transmitir a terceiros, sem prévia autorização por escrito, informação, dados pessoais ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual;

10.6.1. Caso autorizada transmissão de dados pela **DETENTORA** a terceiros, as informações fornecidas/compartilhadas devem se limitar ao estritamente necessário para o fiel desempenho da execução do instrumento contratual.

10.7. A **DETENTORA** deverá adotar planos de resposta a incidentes de segurança eventualmente ocorridos durante o tratamento dos dados coletados para a execução das finalidades desta ATA de Registro de Preços, bem como dispor de mecanismos que possibilitem a sua remediação, de modo a evitar ou minimizar eventuais danos aos titulares dos dados;

10.8. A **DETENTORA** deverá comunicar formalmente e de imediato ao município de Hortolândia, por meio do Gestor da ATA de Registro de Preços, a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a Titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções;

10.8.1. A comunicação acima mencionada não eximirá a **DETENTORA** das obrigações, e/ou sanções que possam incidir em razão da perda de informação, dados pessoais e/ou base de dados.

10.9. Encerrada a vigência da ATA de Registro de Preços ou após a satisfação da finalidade



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

pretendida, a **DETENTORA** interromperá o tratamento dos dados pessoais disponibilizados pelo município de Hortolândia e, em no máximo trinta dias, sob instruções e na medida do determinado por este, eliminará completamente os Dados Pessoais e todas as cópias por ventura existentes (seja em formato digital ou físico), salvo quando a **DETENTORA** tenha que manter os dados para cumprimento de obrigação legal;

10.10. A **DETENTORA** ficará obrigada a assumir total responsabilidade e ressarcimento por todo e qualquer dano e/ou prejuízo sofrido incluindo sanções aplicadas pela autoridade nacional decorrentes de tratamento inadequado dos dados pessoais compartilhados pelo município de Hortolândia para as finalidades pretendidas nesta ATA de Registro de Preços;

10.11. A **DETENTORA** ficará obrigada a assumir total responsabilidade pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados compartilhados pelo município de Hortolândia.

10.11.1. Eventuais responsabilidades serão apuradas de acordo com o que dispõe o [Capítulo VI, Seção III, da LGPD](#).

CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

11.1. Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. As infrações e sanções administrativas serão consideradas e aplicadas nos termos do [Decreto Municipal 5.181 de 24 de janeiro de 2023](#).

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

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO DA ATA DE REGISTRO DE PREÇOS

13.1. A ATA de Registro de Preços se extingue quando vencido o prazo nela estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

13.2. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a contratação pretendida, desde que devidamente motivada.

13.3. A ATA de Registro de Preços pode ser extinta antes de cumpridas as obrigações nela estipuladas, ou antes do prazo nela fixado, por algum dos motivos previstos no [artigo 137 da Lei nº 14.133/2021](#), bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.3.1. Nesta hipótese, aplicam-se também os artigos [138](#) e [139](#) da mesma Lei.

13.4. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir a ATA de Registro de Preços.

13.4.1. Se a operação implicar mudança da pessoa jurídica **DETENTORA**, deverá ser formalizado termo aditivo para alteração subjetiva.

CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Programa, na dotação abaixo discriminada:

01.02.04.131.0201.2.008.339040.01.1100000 - Secretaria de Governo

02.02.04.126.0219.2.015.449040.01.1100000 – SMPUGE

03.01.03.092.0204.2.017.339040.01.1100000 - Secretaria de Assuntos Jurídicos

05.01.04.122.0216.2.020.339040.01.1100000 - Secretaria de Administração

06.01.18.541.0223.2.033.339040.01.1100000 - Secretaria de Meio Ambiente

07.02.06.181.0224.2.041.339040.01.1000074 - Secretaria de Segurança

08.01.22.661.0225.2.043.339040.01.1100000 - Secretaria de Desenv. Econômico

09.01.15.452.0220.2.046.339040.01.1100000 - Secretaria de Serviços Urbanos



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

10.01.15.452.0226.2.051.339040.01.1100000 - Secretaria de Mobilidade Urbana

11.01.16.482.0227.2.055.339040.01.1100000 - Secretaria de Habitação

12.01.08.244.0207.2.058.339040.01.5100000 - Secretaria de Inclusão Social

13.01.12.122.0209.2.074.339040.01.2200000 - Secretaria de Educação

14.01.15.451.0230.2.103.339040.01.1100000 - Secretaria de Obras

15.01.10.122.0212.2.104.339040.01.3100000 - Secretaria de Saúde

16.01.13.392.0228.2.131.339040.01.1100000 - Secretaria de Cultura

17.01.27.812.0229.2.136.339040.01.1100000 - Secretaria de Esportes

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1. Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na [Lei nº 14.133, de 2021](#), e demais normas aplicáveis e, subsidiariamente, segundo as disposições contidas na [Lei nº 8.078, de 1990 – Código de Defesa do Consumidor](#) – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos [arts. 124 e seguintes da Lei nº 14.133, de 2021](#).

16.2. A **DETENTORA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, nos termos do [art. 125 da Lei Federal 14.133/2021](#).

16.3. Registros que não caracterizam alteração da ATA de Registro de Preços podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do [art. 136 da Lei nº 14.133, de 2021](#).

CLÁUSULA DÉCIMA SÉTIMA – DO TERMO CONTRATUAL

17.1. As obrigações decorrentes desta ATA de Registro de Preços poderão ser formalizadas



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

através de termo contratual, podendo ainda consubstanciar-se na própria nota de empenho, na hipótese prevista no [artigo 95 da Lei Federal nº 14.133/2021 e suas alterações](#).

17.2. A recusa da **DETENTORA** em retirar a nota de empenho ou assinar o contrato, ambos decorrentes desta ATA de Registro de Preços, caracteriza descumprimento de obrigações, podendo-lhe acarretar as sanções previstas.

17.3. No caso previsto no subitem anterior, a critério da Administração, poderá ser celebrada a ATA de Registro de Preços com as remanescentes, obedecida à ordem classificatória e as mesmas condições oferecidas pela **DETENTORA**, inclusive quanto ao preço.

CLÁUSULA DÉCIMA OITAVA – PUBLICAÇÃO

18.1. Incumbirá ao **CONTRATANTE** divulgar o presente instrumento no [Portal Nacional de Contratações Públicas \(PNCP\)](#), na forma prevista no [art. 94 da Lei 14.133, de 2021](#), bem como no respectivo sítio oficial na Internet, em atenção ao [art. 8º, §2º, da Lei n. 12.527, de 2011](#), c/c [art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012](#).

CLÁUSULA DÉCIMA NONA – FORO

19.1. A interpretação e aplicação dos termos contratuais serão regidas pelas leis brasileiras e o Juízo da Comarca de Hortolândia – Estado de São Paulo, terá jurisdição e competência sobre qualquer controvérsia resultante desta ATA de Registro de Preços, constituindo assim o foro de eleição, prevalecendo sobre qualquer outro, por mais privilegiado que seja.

E, por estarem assim justas e acordadas, as partes assinam a presente, por si e seus sucessores, para todos os fins de direito.

MUNICÍPIO DE HORTOLÂNDIA
«SEC_REQUISITANTE»
«Nome_Secretária»



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

«DETENTORA»

«NOME_RESP_LEGAL»



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

ANEXO V

Minuta de Termo de Contrato

MUNICÍPIO DE HORTOLÂNDIA

PROCESSO ADMINISTRATIVO Nº 100876/2025

CONTRATO Nº «CRT», RESULTANTE DO PREGÃO ELETRÔNICO Nº ____/2026, QUE FAZEM ENTRE SI O MUNICÍPIO DE HORTOLÂNDIA, POR INTERMÉDIO DO (A) «SEC_REQUISITANTE», E «**CONTRATADA**».

O **MUNICÍPIO DE HORTOLÂNDIA**, pessoa jurídica de direito público interno, sediada na Rua Professora Celina Franceschini Bueno, nº 100, Bairro Jardim Metropolitano, no Município de Hortolândia – SP, cadastrada junto ao Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda (CNPJ/MF) sob nº 67.995.027/0001-32, neste ato, representado pelo(a) Secretário(a) Municipal, Sr.(a) «**Nome_Secretárioa**», «Dados_Secretário», doravante denominado **CONTRATANTE**, e, de outro lado, a empresa «**CONTRATADA**», pessoa jurídica de direito privado, sediada na «END_LOGRADOURO», «N_COMPL», Bairro «BAIRRO», CEP: «CEP», no Município de «CIDADE», Estado de «ESTADO», cadastrada junto ao Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda – (CNPJ/MF) sob o nº «CNPJ», com Inscrição Estadual registrada sob nº «IE», neste ato representado por seu «CARGO_RESP_LEGAL» Sr. «**NOME_RESP_LEGAL**», «NACIONALIDADE», «ESTADO_CIVIL», «QUALIFICAÇÃO_PROFISSIONAL», portador da Cédula de Identidade (R.G.) nº «RG_C_UF_EMISSOR», devidamente inscrito junto ao Cadastro de Pessoas Físicas do Ministério da Fazenda – (CPF/MF) sob nº «CPF», doravante denominada **CONTRATADA**, firmam o presente **CONTRATO**, mediante as cláusulas e condições a seguir



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

enunciadas.

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia, de acordo com as especificações contidas no Termo de referência, e nas demais condições aqui estipuladas.

1.2. Objeto da contratação:

ITEM	CÓDIGO	QTDE	UN.	DESCRIÇÃO	MARCA	VALOR UNIT	VALOR TOTAL
01	12.3.3929	02	Un	Firewall tipo 1			
02	12.3.3930	30	Un	Firewall tipo 2			
03	12.3.3931	110	Un	Firewa ll tipo 3			
04	12.3.3932	01	Un	Solução de Gerenciamento Centralizado e relatório NGFW Tipos 1, 2 e 3			
05	12.3.3933	70	Un	Solução para acesso seguro à aplicação privada e ZTNA			
06	12.3.3939	01	Serv.	Treinamento para a solução Firewall			

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A ATA de Registro de Preços nº ____/2025;

1.3.4. A Proposta da **CONTRATADA**;

1.3.5. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência deste contrato será de __ (____) ____, contados da **assinatura digital qualificada** deste instrumento, podendo ser prorrogado nos termos da legislação



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

vigente.

2.1.1. Este contrato poderá ser assinado:

2.1.1.1. Por meio de **assinatura digital qualificada**, caso em que o **termo inicial da vigência** (primeiro dia de vigência) corresponderá à data da assinatura deste instrumento, considerando-se, para tanto, o momento em que a última parte signatária formalizar sua assinatura eletrônica, nos termos da [Medida Provisória nº 2.200-2/2001](#) e demais normas regulamentares pertinentes; ou

2.1.1.2. Por meio de **assinatura física**, por ambas as partes, caso em que o **termo inicial da vigência** será a data constante ao final deste contrato.

2.1.2. O **termo final da vigência** (último dia de vigência) dar-se-á no mesmo dia do mês em que se iniciou a vigência, após o decurso do período estipulado no contrato, conforme especificado no item 2.1.1, ressalvada a possibilidade de prorrogação, observadas as formalidades legais e as condições ajustadas entre as partes.

2.1.3. A assinatura eletrônica, conforme regulamentação vigente, equipara-se à assinatura manuscrita para todos os efeitos legais, garantindo a validade, autenticidade e integridade deste instrumento.

2.2. As prorrogações de prazo de vigência serão formalizadas mediante celebração dos respectivos termos de aditamento, respeitadas as condições prescritas na [Lei Federal nº 14.133/2021](#).

2.3. Não serão considerados como inadimplemento contratual os atrasos provocados por motivos de comprovada força maior ou caso fortuito, desde que notificados no prazo de 48 (quarenta e oito) horas após o evento e aceitos pelo **CONTRATANTE**.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

de Referência, anexo a este contrato.

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA – PREÇO

5.1. O valor total do presente contrato é de R\$ (.....).

5.2. 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.

CLÁUSULA SEXTA – PAGAMENTO

6.1. A **CONTRATADA**, quando do cumprimento das Autorizações de Fornecimento, emitirá as respectivas notas fiscais/faturas, discriminando as quantidades e produtos fornecidos.

6.2. Após a efetiva entrega e conferência dos itens, o (s) profissional (is) responsável (is) promoverá (ão) o ateste na (s) nota (s) fiscal (is), encaminhando-as para pagamento.

6.3. Os pagamentos deverão ser efetuados em 10 (dez) dias, fora a dezena, da data do ateste das notas fiscais/faturas.

6.4. As notas fiscais/fatura deverão ser emitidas para o **MUNICÍPIO DE HORTOLÂNDIA**, sob o número de **CNPJ 67.995.027/0001-32**.

6.5. Quando as Autorizações de fornecimento forem emitidas pela Secretaria Municipal de Saúde, as notas fiscais/fatura deverão ser emitidas para o **FUNDO MUNICIPAL DE SAÚDE**, sob o número de **CNPJ 13.843.145/0001-04**.

6.6. Por força da [Instrução Normativa RFB nº 2043/2021](#), para fins Tributários, os valores para recolhimento previdenciário (INSS) devem estar discriminados na Nota Fiscal;

6.7. Considerando decisão proferida pelo STF – RE 1.293.453 em 11/10/2021 e por força



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

do [Decreto Municipal 4.947/2021](#) que trata das regras de retenção de tributos no pagamento a fornecedores por Órgãos e Entidades do Poder Executivo, dispostas na [Instrução Normativa RFB nº 1234/2012](#), ao efetuar os pagamentos a **CONTRATANTE** procederá à retenção do imposto de renda (IR).

6.7.1. As retenções serão realizadas no momento do pagamento dos valores decorrentes da prestação de serviços contratados ou fornecimento dos bens contratados, uma vez atestados e liquidados, mediante recolhimento aos cofres municipais, nos termos do [inciso I do art. 158 da Constituição Federal de 1988](#);

6.7.2. As retenções serão efetuadas sobre qualquer forma de pagamento, inclusive os pagamentos antecipados por conta de fornecimento de bens ou prestação de serviços, para entrega futura;

6.7.3. Não estão sujeitos à retenção do IR na fonte os pagamentos realizados a pessoas ou serviços e mercadorias elencados no [art. 4º da Instrução Normativa RFB nº 1234, de 11 de janeiro de 2012](#).

6.8. Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido de alguma forma, deverá ser acrescido de encargos moratórios proporcionais aos dias de atraso, apurados desde a data limite prevista para o pagamento até a data do efetivo pagamento, à taxa de 6% (seis por cento) ao ano, aplicando-se a seguinte fórmula:

$$EM = I \times N \times VP$$

EM = Encargos Moratórios a serem acrescidos ao valor originariamente devido

I = Índice de atualização financeira, calculado segundo a fórmula:

$$I = \frac{(6 / 100)}{365}$$



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

N = Número de dias entre a data limite prevista para o pagamento e a data do efetivo pagamento

VP = Valor da Parcela em atraso

CLÁUSULA SÉTIMA – REAJUSTE

7.1. Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data do orçamento estimado.

7.1.1. A data base do orçamento estimado é _____.

7.2. Após o intervalo de um ano, os preços poderão ser reajustados após negociação entre as partes, observando-se como limite máximo a variação do índice IPCA/IBGE.

7.3. O reajuste de preços deverá ser solicitado formalmente pela **CONTRATADA**.

7.4. Para a concessão do reajuste deverá ser comprovado que a **CONTRATADA** não concorreu para que o prazo inicialmente pactuado não tenha sido cumprido.

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

7.6. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o **CONTRATANTE** pagará à **CONTRATADA** a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.7. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.8. 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.

7.9. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.10. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA – OBRIGAÇÕES DO CONTRATANTE

8.1. Sem prejuízo das obrigações descritas no Termo de referências, são obrigações da **CONTRATANTE**:

8.2. Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com o contrato e seus anexos;

8.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

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

8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela **CONTRATADA**;

8.6. Comunicar a empresa 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, de 2021](#);

8.7. Efetuar o pagamento a **CONTRATADA** do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente contrato;

8.8. Aplicar a **CONTRATADA** as sanções previstas na lei e neste contrato;

8.9. Cientificar o órgão de representação judicial da Prefeitura Municipal de Hortolândia para adoção das medidas cabíveis quando do descumprimento de obrigações pela **CONTRATADA**;

8.10. Explicitamente emitir decisão sobre todas 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



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

ajuste.

8.10.1. A Administração terá o prazo de 01 (um) mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela **CONTRATADA** no prazo máximo de 01 (um) mês.

8.12. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.13. 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 da **CONTRATADA**, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATADA

9.1. Sem prejuízo das obrigações descritas no Termo de referências, são obrigações da **CONTRATADA**:

9.2. A **CONTRATADA** deve cumprir todas as obrigações constantes deste contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.3. Comunicar ao **CONTRATANTE**, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.4. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior ([art. 137, II, da Lei n.º 14.133, de 2021](#)) e prestar todo esclarecimento ou informação por eles solicitados;

9.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

- 9.6.** Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução do contrato pela **CONTRATANTE**, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;
- 9.7.** Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao **CONTRATANTE** e não poderá onerar o objeto do contrato;
- 9.8.** Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto.
- 9.9.** Paralisar, por determinação do **CONTRATANTE**, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
- 9.10.** Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;
- 9.11.** Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação ([art. 116, da Lei n.º 14.133, de 2021](#));
- 9.12.** Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas ([art. 116, parágrafo único, da Lei n.º 14.133, de 2021](#));
- 9.13.** Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
- 9.14.** 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



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

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, de 2021](#).

9.15. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do **CONTRATANTE**;

9.16. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, 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;

9.17. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.

9.18. Submeter previamente, por escrito, ao **CONTRATANTE**, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

9.19. Não permitir a utilização de qualquer trabalho do menor de dezesesseis 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.

9.20. Observar e seguir à risca, a todas as disposições contidas no Manual de boas-vindas para prestadores de serviço, anexo a este contrato.

CLÁUSULA DÉCIMA – LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

10.1. As partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, nos termos da Lei Geral de Proteção de Dados – LGPD ([Lei nº 13.709, de 14 de agosto de 2018](#));

10.1.1. O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos artigos [7º](#), [11](#) e/ou [14](#) da [Lei nº 13.709/2018](#) às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

informados ao titular.

10.2. A **CONTRATADA** obriga-se ao dever de proteção, confidencialidade, sigilo de toda informação, dados pessoais e base de dados a que tiver acesso, nos termos da LGPD, suas alterações e regulamentações posteriores, durante o cumprimento do objeto descrito no instrumento contratual;

10.2.1. A **CONTRATADA** não poderá se utilizar de informação, dados pessoais ou base de dados a que tenham acesso, para fins distintos da execução dos serviços especificados no instrumento contratual;

10.2.2. Em caso de necessidade de coleta de dados pessoais dos titulares mediante consentimento, indispensáveis à própria prestação do serviço, esta será realizada após prévia aprovação do município de Hortolândia, responsabilizando-se a **CONTRATADA** pela obtenção e gestão.

10.3. A **CONTRATADA** obriga-se a implementar medidas técnicas e administrativas aptas a promover a segurança, a proteção, a confidencialidade e o sigilo de toda informação, dados pessoais e/ou base de dados que tenha acesso, a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito; tudo isso de forma a reduzir o risco ao qual o objeto do contrato ou o município de Hortolândia está exposto;

10.4. A **CONTRATADA** deverá manter os registros de tratamento de dados pessoais que realizar, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer tempo;

10.4.1. A **CONTRATADA** deverá permitir a realização de auditorias do município de Hortolândia e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações relacionadas à sistemática de proteção de dados;

10.4.2. A **CONTRATADA** deverá apresentar ao município de Hortolândia, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados na contratação, de forma



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

a assegurar a auditabilidade do objeto contratado, bem como os demais dispositivos legais aplicáveis.

10.5. A CONTRATADA se responsabilizará por assegurar que todos os seus colaboradores, consultores, e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo, devendo estes assumir compromisso formal de preservar a confidencialidade e segurança de tais dados, documento que deverá estar disponível em caráter permanente para exibição ao município de Hortolândia, mediante solicitação;

10.5.1. A CONTRATADA deverá promover a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do município de Hortolândia, em caso de desligamento de funcionário das atividades inerentes à execução do presente contrato.

10.6. A CONTRATADA não poderá disponibilizar ou transmitir a terceiros, sem prévia autorização por escrito, informação, dados pessoais ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual;

10.6.1. Caso autorizada transmissão de dados pela **CONTRATADA** a terceiros, as informações fornecidas/compartilhadas devem se limitar ao estritamente necessário para o fiel desempenho da execução do instrumento contratual.

10.7. A CONTRATADA deverá adotar planos de resposta a incidentes de segurança eventualmente ocorridos durante o tratamento dos dados coletados para a execução das finalidades deste contrato, bem como dispor de mecanismos que possibilitem a sua remediação, de modo a evitar ou minimizar eventuais danos aos titulares dos dados;

10.8. A CONTRATADA deverá comunicar formalmente e de imediato ao município de Hortolândia, por meio do Gestor do contrato, a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a Titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções;

10.8.1. A comunicação acima mencionada não eximirá a **CONTRATADA** das



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

obrigações, e/ou sanções que possam incidir em razão da perda de informação, dados pessoais e/ou base de dados.

10.9. Encerrada a vigência do contrato ou após a satisfação da finalidade pretendida, a **CONTRATADA** interromperá o tratamento dos dados pessoais disponibilizados pelo município de Hortolândia e, em no máximo trinta dias, sob instruções e na medida do determinado por este, eliminará completamente os Dados Pessoais e todas as cópias por ventura existentes (seja em formato digital ou físico), salvo quando a **CONTRATADA** tenha que manter os dados para cumprimento de obrigação legal;

10.10. A **CONTRATADA** ficará obrigada a assumir total responsabilidade e ressarcimento por todo e qualquer dano e/ou prejuízo sofrido incluindo sanções aplicadas pela autoridade nacional decorrentes de tratamento inadequado dos dados pessoais compartilhados pelo município de Hortolândia para as finalidades pretendidas neste contrato;

10.11. A **CONTRATADA** ficará obrigada a assumir total responsabilidade pelos danos patrimoniais, morais, individuais ou coletivos que venham a ser causados em razão do descumprimento de suas obrigações legais no processo de tratamento dos dados compartilhados pelo município de Hortolândia.

10.11.1. Eventuais responsabilidades serão apuradas de acordo com o que dispõe o [Capítulo VI, Seção III, da LGPD](#).

CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

11.1. Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. As infrações e sanções administrativas serão consideradas e aplicadas nos termos do [Decreto Municipal 5.181 de 24 de janeiro de 2023](#).

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

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO DO CONTRATO



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

13.1. O contrato se extingue quando cumpridas as obrigações de ambas as partes.

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

13.2.1. Nesta hipótese, aplicam-se também os artigos [138](#) e [139](#) da mesma Lei.

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

13.3.1. Se a operação implicar mudança da pessoa jurídica **CONTRATADA**, deverá ser formalizado termo aditivo para alteração subjetiva.

13.4. O termo de rescisão, sempre que possível, será precedido de:

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

13.4.2. Relação dos pagamentos já efetuados e ainda devidos;

13.4.3. Indenizações e multas.

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

CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Programa, na dotação abaixo discriminada:

01.02.04.131.0201.2.008.339040.01.1100000 - Secretaria de Governo

02.02.04.126.0219.2.015.449040.01.1100000 – SMPUGE

03.01.03.092.0204.2.017.339040.01.1100000 - Secretaria de Assuntos Jurídicos

05.01.04.122.0216.2.020.339040.01.1100000 - Secretaria de Administração



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

06.01.18.541.0223.2.033.339040.01.1100000 - Secretaria de Meio Ambiente

07.02.06.181.0224.2.041.339040.01.1000074 - Secretaria de Segurança

08.01.22.661.0225.2.043.339040.01.1100000 - Secretaria de Desenv. Econômico

09.01.15.452.0220.2.046.339040.01.1100000 - Secretaria de Serviços Urbanos

10.01.15.452.0226.2.051.339040.01.1100000 - Secretaria de Mobilidade Urbana

11.01.16.482.0227.2.055.339040.01.1100000 - Secretaria de Habitação

12.01.08.244.0207.2.058.339040.01.5100000 - Secretaria de Inclusão Social

13.01.12.122.0209.2.074.339040.01.2200000 - Secretaria de Educação

14.01.15.451.0230.2.103.339040.01.1100000 - Secretaria de Obras

15.01.10.122.0212.2.104.339040.01.3100000 - Secretaria de Saúde

16.01.13.392.0228.2.131.339040.01.1100000 - Secretaria de Cultura

17.01.27.812.0229.2.136.339040.01.1100000 - Secretaria de Esportes

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1. Os casos omissos serão decididos pelo **CONTRATANTE**, segundo as disposições contidas na [Lei nº 14.133, de 2021](#), e demais normas aplicáveis e, subsidiariamente, segundo as disposições contidas na [Lei nº 8.078, de 1990 – Código de Defesa do Consumidor](#) – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos [arts. 124 e seguintes da Lei nº 14.133, de 2021](#).

16.2. A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, nos termos do [art. 125 da Lei Federal 14133/2021](#).

16.3. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do [art. 136 da Lei nº 14.133, de 2021](#).

CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao **CONTRATANTE** divulgar o presente instrumento no [Portal Nacional de Contratações Públicas \(PNCP\)](#), na forma prevista no [art. 94 da Lei 14.133, de 2021](#), bem como no respectivo sítio oficial na Internet, em atenção ao [art. 8º, §2º, da Lei n. 12.527, de 2011](#), c/c [art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012](#).

CLÁUSULA DÉCIMA OITAVA – AMPARO LEGAL

18.1. O presente Contrato Administrativo é regido pelas disposições contidas na [Lei Federal nº 14.133/2021](#), suas alterações e demais normas complementares de direito privado e disposições deste instrumento, bem como as disposições contidas no Processo Administrativo protocolado sob nº 100876/2025, originário do Procedimento Licitatório instaurado na modalidade de Pregão Eletrônico nº ____/2026, seus Anexos, tudo fazendo parte integrante do presente instrumento contratual, como se no mesmo transcritos fossem.

CLÁUSULA DÉCIMA NONA – FORO

19.1. A interpretação e aplicação dos termos contratuais serão regidas pelas leis brasileiras e o Juízo da Comarca de Hortolândia – Estado de São Paulo, terá jurisdição e competência sobre qualquer controvérsia resultante deste contrato, constituindo assim o foro de eleição, prevalecendo sobre qualquer outro, por mais privilegiado que seja.



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

E, por estarem assim justas e acordadas, as partes assinam a presente, por si e seus sucessores, para todos os fins de direito.

MUNICÍPIO DE HORTOLÂNDIA

«Nome_Secretárioa»

«CONTRATADA»

«NOME_RESP_LEGAL»



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

ANEXO VI

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: **MUNICÍPIO DE HORTOLÂNDIA**

CONTRATADO: **«CONTRATADA»**

CONTRATO Nº (DE ORIGEM): **«CRT»**

OBJETO: _____

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

- a)** O ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo tribunal de contas do estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;
- b)** Poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, despachos e decisões, mediante regular cadastramento no sistema de processo eletrônico, em consonância com o estabelecido na resolução nº 01/2011 do TCESP;
- c)** Além de disponíveis no processo eletrônico, todos os despachos e decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no diário oficial do estado, caderno do poder legislativo, parte do tribunal de contas do estado de São Paulo, em conformidade com o artigo 90 da lei complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do código de processo civil;
- d)** As informações pessoais dos responsáveis pela contratante e interessados estão cadastradas no módulo eletrônico do “cadastro corporativo tcesp – cadtcesp”, nos termos previstos no artigo 2º das instruções nº01/2020, conforme “declaração(ões) de atualização cadastral” anexa (s);
- e)** É de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

2. Damo-nos por notificados para:



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

- a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;
- b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

LOCAL e DATA: _____

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:

Nome: _____

Cargo: _____

CPF: _____

**RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME OU RATIFICAÇÃO DA
DISPENSA/INEXIGIBILIDADE DE LICITAÇÃO:**

Nome: «Nome_Secretária»

Cargo: _____

CPF: _____

Assinatura: _____

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:

Pelo contratante:

Nome: «Nome_Secretária»

Cargo: _____

CPF: _____

Assinatura: _____

Pela contratada:

Nome: «NOME_RESP_LEGAL»

Cargo: «CARGO_RESP_LEGAL»



PREFEITURA MUNICIPAL DE HORTOLÂNDIA

CPF: «CPF»

Assinatura: _____

ORDENADOR DE DESPESAS DA CONTRATANTE:

Nome: «Nome_Secretária»

Cargo: _____

CPF: _____

Assinatura: _____

GESTOR(ES) DO CONTRATO:

Nome: _____

Cargo: _____

CPF: _____

Assinatura: _____

DEMAIS RESPONSÁVEIS (*):

Tipo de ato sob sua responsabilidade: _____

Nome: _____

Cargo: _____

CPF: _____

Assinatura: _____

(*) - O Termo de Ciência e Notificação e/ou Cadastro do(s) Responsável(is) deve identificar as pessoas físicas que tenham concorrido para a prática do ato jurídico, na condição de ordenador da despesa; de partes contratantes; de responsáveis por ações de acompanhamento, monitoramento e avaliação; de responsáveis por processos licitatórios; de responsáveis por prestações de contas; de responsáveis com atribuições previstas em atos legais ou administrativos e de interessados relacionados a processos de competência deste Tribunal. Na hipótese de prestações de contas, caso o signatário do parecer conclusivo seja distinto daqueles já arrolados como subscritores do Termo de Ciência e Notificação, será ele objeto de notificação específica. (inciso acrescido pela Resolução nº 11/2021).