AVISO DE CONTRATAÇÃO DIRETA

Processo Administrativo n.° 1.520/2024

Torna-se público que o **SEPREV – Serviço de Previdência e Assistência à Saúde dos Servidores Municipais de Indaiatuba**, por intermédio do Departamento Administrativo, realizará uma Dispensa de Licitação, com critério de julgamento de **menor preço**, conforme previsto no art. 75, inciso II, da Lei nº 14.133, de 1º de abril de 2021, e nas disposições contidas na Lei Complementar nº 123/2006, na Lei Complementar nº 147/2014, no Decreto Municipal nº 14.958/2023 e na Portaria nº 174/2021.

Data Limite para Apresentação das Propostas: 09 de setembro de 2024 às 17h.

Endereço Eletrônico Para Envio das Propostas e Documentação: thaiane.almeida@seprev.sp.gov.br.

1. DO OBJETO, CONDIÇÕES DE PARTICIPAÇÃO E ESTIMATIVA DE VALOR

1.1. O objeto do presente procedimento é a escolha da proposta mais vantajosa para a contratação de solução integrada de Firewall Next Generation, com sistema redundante em alta disponibilidade, contemplando o fornecimento de equipamentos e de licenças, para prevenção de ataques cibernéticos e proteção dos dados e informações dos computadores e servidores de arquivos do SEPREV, por um período de 12 (doze) meses, conforme condições, quantidades e exigências estabelecidas neste Aviso de Contratação Direta e seus anexos.

1.2. A contratação será em lote único, conforme tabela constante abaixo:

Lote	Especificação	Unidade	Quantidade
01	Contratação de solução integrada de Firewall Next Generation, com sistema redundante em alta disponibilidade, contemplando o fornecimento de equipamentos e de licenças, para prevenção de ataques cibernéticos e proteção dos dados/informações dos computadores e servidores de arquivos do SEPREV.	Serviço	01

1.2.1. O Lote 1, que compreende a solução integrada de Firewall Next Generation, objeto dessa licitação, deve conter, ao menos, os seguintes itens, com suas respectivas configurações mínimas:

ITEM	DESCRIÇÃO
1	APPLIANCE UTM de 10 Gbps de capacidade de firewall – alta disponibilidade por meio de equipamentos redundantes (2 - dois)
2	SOLUÇÃO DE GERENCIAMENTO WEB DE FIREWALL e ARMAZENAMENTO DE LOG POR 12 (DOZE) MESES EM NUVEM DO FABRICANTE COM AS LICENÇAS DE USO NECESSÁRIAS PARA

	ATENDIMENTO INTEGRAL DOS REQUISITOS PREVISTOS NESTE DOCUMENTO
3	SERVIÇO DE INSTALAÇÃO
4	TREINAMENTO PARA O SISTEMA DE FIREWALL UTM HANDS-ON
5	SERVIÇOS DE PRESTAÇÃO DE SUPORTE TÉCNICO REMOTO (NOC) 10X5 NA SOLUÇÃO COM HORAS ILIMITADAS E MONITORAMENTO 24X7.

1.2.1.1. **O detalhamento de todos os itens está descrito no Anexo II deste Aviso de Contratação Direta.**

1.3. O critério de julgamento adotado será o menor preço, observadas as exigências contidas neste Aviso de Contratação Direta e seus Anexos quanto às especificações do objeto.

1.4. Início da execução do objeto: Conforme Termo de Referência – Anexo I.

1.5. Os serviços, objeto da contratação, serão realizados na Sede do SEPREV, na Rua dos Ipês, nº 125, Jardim Pompéia, Indaiatuba/SP.

1.6. O valor total estimado para a presente contratação é de **R$ 29.132,40 (vinte e nove mil cento e trinta e dois reais e quarenta centavos).**

1.7. 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 e do Decreto n.º 8.538, de 2015.

1.8. Não poderão participar desta dispensa de licitação os fornecedores:

1.8.1. Que não atendam às condições deste Aviso de Contratação Direta e seu(s) anexo(s);

1.8.2. Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

1.8.3. Que se enquadrem nas seguintes vedações:

a) autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ele relacionados;

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

c) pessoa física ou jurídica que se encontre, ao tempo da contratação, impossibilitada de contratar em decorrência de sanção que lhe foi imposta;

d) 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 dispensa de 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;

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

f) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do aviso, 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.

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

1.8.4.1. O disposto na alínea "c" aplica-se também ao fornecedor 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 fornecedor;

1.8.5. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário); e

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

2. JULGAMENTO E ACEITAÇÃO DAS PROPOSTAS

2.1. Encerrado o prazo para envio de propostas, quando a proposta do primeiro colocado permanecer acima do preço máximo ou abaixo do desconto definido para a contratação, o agente de contratação poderá negociar condições mais vantajosas.

2.1.1. Neste caso, será encaminhada contraproposta ao fornecedor que tenha apresentado o menor preço ou o maior desconto, para que seja obtida a melhor proposta compatível em relação ao estipulado pela Administração.

2.1.2. A negociação poderá ser feita com os demais fornecedores classificados, respeitada a ordem de classificação, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo ou abaixo do desconto definido para a contratação.

2.2. Em qualquer caso, concluída a negociação, se houver, o resultado será divulgado a todos e registrado no procedimento da dispensa, devendo esta ser anexada aos autos do processo de contratação.

2.3. Constatada a compatibilidade entre o valor da proposta e o estipulado para a contratação, será solicitado ao fornecedor o envio da proposta adequada ao valor negociado, se for o caso, acompanhada dos documentos complementares, quando necessários.

2.4. Encerrada a etapa de negociação, se houver, o agente de contratação verificará se o fornecedor provisoriamente classificado em primeiro lugar atende às

condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e neste Aviso, especialmente quanto à existência de sanção que impeça a participação no processo de contratação direta ou a futura contratação, mediante a consulta aos seguintes cadastros:

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

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

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

2.5.1. Constatada a existência de sanção, o fornecedor será reputado inabilitado, por falta de condição de participação.

2.6. Verificadas as condições de participação, o gestor 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 Aviso de Contratação Direta e em seus anexos.

2.7. Será desclassificada a proposta vencedora que:

2.7.1. contiver vícios insanáveis;

2.7.2. não obedecer às especificações técnicas pormenorizadas neste aviso ou em seus anexos;

2.7.3. não tiver sua exequibilidade demonstrada, quando exigido pela Administração;

2.7.4. apresentar desconformidade com quaisquer outras exigências deste aviso ou seus anexos, desde que insanável.

2.8. Quando o fornecedor não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços que:

2.8.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da dispensa não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio fornecedor, para os quais ele renuncie a parcela ou à totalidade da remuneração.

2.8.2. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

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

2.10. 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.

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

2.10.2. 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.

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

2.12. Se a proposta vencedora for desclassificada, será examinada a proposta subsequente, e, assim sucessivamente, na ordem de classificação.

2.13. Encerrada a análise quanto à aceitação da proposta, será iniciada a fase de habilitação, observado o disposto neste Aviso de Contratação Direta.

3. HABILITAÇÃO

3.1. Os documentos a serem exigidos para fins de habilitação, constam do Termo de Referência e serão solicitados do fornecedor mais bem classificado.

3.1.1. O descumprimento do item acima implicará a inabilitação do fornecedor, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões lograr êxito em encontrar a(s) certidão(ões) válida(s).

3.2. O objeto social constante em contrato deverá ser compatível com o objeto pertinente e constante deste Aviso de Contratação.

3.3. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não digitais quando houver dúvida em relação à integridade do documento digital.

3.4. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

3.5. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

3.6. Será inabilitado o fornecedor que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Aviso de Contratação Direta.

3.6.1. Na hipótese de o fornecedor não atender às exigências para a habilitação, o órgão ou entidade examinará a proposta subsequente, e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às especificações do objeto e as condições de habilitação

3.7. Constatado o atendimento às exigências de habilitação, o fornecedor será habilitado.

4. CONTRATAÇÃO

4.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

4.2. O adjudicatário terá o prazo de até 10 (dez) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato **OU** aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Aviso de Contratação Direta.

4.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida ao fornecedor adjudicado, implica o reconhecimento de que:

4.3.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

4.3.2. a contratada se vincula à sua proposta e às previsões contidas no Aviso de Contratação Direta e seus anexos;

4.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133, de 2021 e reconhece os direitos da Administração previstos nos artigos 137 a 139 da mesma Lei.

4.4. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

4.5. Na assinatura do contrato ou do instrumento equivalente será exigida a comprovação das condições de habilitação e contratação consignadas neste aviso, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

5. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

5.1. Comete infração administrativa o fornecedor que praticar quaisquer das hipóteses previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

5.1.1. dar causa à inexecução parcial do contrato;

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

5.1.3. dar causa à inexecução total do contrato;

5.1.4. deixar de entregar a documentação exigida para o certame;

5.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

5.1.7. ensejar o retardamento da execução ou da entrega do objeto da contratação direta sem motivo justificado;

5.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa ou a execução do contrato;

5.1.9. fraudar a dispensa ou praticar ato fraudulento na execução do contrato;

5.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

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

5.1.11. praticar atos ilícitos com vistas a frustrar os objetivos deste certame.

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

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

a) Advertência pela falta do subitem 5.1.1 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

b) Multa de 30% (trinta por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor, por qualquer das infrações dos subitens 5 a 5.1.12;

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 5.1.2 a 5.1.7 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 5.1.8 a 5.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

5.3. A aplicação das sanções previstas neste Aviso de Contratação Direta não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante (art. 156, §9º)

5.4. Todas as sanções previstas neste Aviso poderão ser aplicadas cumulativamente com a multa (art. 156, §7º).

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

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

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

5.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o

procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

5.9. Na aplicação das sanções serão considerados (art. 156, §1º):

5.10. a natureza e a gravidade da infração cometida;

5.11. as peculiaridades do caso concreto;

5.12. as circunstâncias agravantes ou atenuantes;

5.13. os danos que dela provierem para o Contratante;

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

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

5.16. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160)

5.17. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161)

5.18. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

5.19. As sanções por atos praticados no decorrer da contratação estão previstas nos anexos a este Aviso.

6. DAS DISPOSIÇÕES GERAIS

6.1. No caso de todos os fornecedores restarem desclassificados ou inabilitados (procedimento fracassado), a Administração poderá:

6.1.1. republicar o presente aviso com uma nova data;

6.1.2. valer-se, para a contratação, de proposta obtida na pesquisa de preços que serviu de base ao procedimento, se houver, privilegiando-se os menores preços, sempre que possível, e desde que atendidas às condições de habilitação exigidas.

6.1.2.1. No caso do subitem anterior, a contratação será operacionalizada fora deste procedimento.

6.1.3. fixar prazo para que possa haver adequação das propostas ou da documentação de habilitação, conforme o caso.

6.2. As providências dos subitens 6.1.1 e 66.1.2 também poderão ser utilizadas se não houver o comparecimento de quaisquer fornecedores interessados (procedimento deserto).

6.3. Havendo a necessidade de realização de ato de qualquer natureza pelos fornecedores, cujo prazo não conste deste Aviso de Contratação Direta, deverá ser atendido o prazo indicado pelo agente competente da Administração na respectiva notificação.

6.4. Caberá ao fornecedor acompanhar as operações, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pela Administração ou de sua desconexão.

6.5. 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.

6.6. No julgamento das propostas e da habilitação, a Administração poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

6.7. As normas disciplinadoras deste Aviso de Contratação Direta 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.

6.8. Os fornecedores 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 de contratação.

6.9. O SEPREV poderá valer-se, para a contratação, de proposta obtida na pesquisa de preços que serviu de base ao procedimento, se houver, privilegiando os menores preços, sempre que possível, e desde que atendidas as condições de habilitação exigidas.

6.10. Em caso de divergência entre disposições deste Aviso de Contratação Direta e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Aviso.

6.11. Integram este Aviso de Contratação Direta, para todos os fins e efeitos, os seguintes anexos:

a) ANEXO I – Termo de Referência

b) ANEXO II – Especificações do Objeto

c) ANEXO III – Minuta Contratual

Indaiatuba, aos 04 de setembro de 2024.

Thaiane Aparecida dos Santos Almeida
Analista Técnico Administrativo

ANEXO I – TERMO DE REFERÊNCIA

Processo Administrativo nº. 1.520/2024

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 Contratação de solução integrada de Firewall Next Generation, com sistema redundante em alta disponibilidade, contemplando o fornecimento de equipamentos e de licenças, para prevenção de ataques cibernéticos e proteção dos dados e informações dos computadores e servidores de arquivos do SEPREV.

1.2 **Da Especificação do Objeto:**

Lote	Especificação	Unidade	Quantidade
01	Contratação de solução integrada de Firewall Next Generation, com sistema redundante em alta disponibilidade, contemplando o fornecimento de equipamentos e de licenças, para prevenção de ataques cibernéticos e proteção dos dados/informações dos computadores e servidores de arquivos do SEPREV.	Serviço	01

1.3 Os bens objeto desta contratação são caracterizados como comuns, conforme os padrões de desempenho e qualidade podem ser objetivamente definidos, por meio de especificações usuais de mercado.

1.4 O prazo de vigência do Contrato é de 12 (doze) meses contados da assinatura, prorrogável na forma da Lei nº 14.133/2021.

1.5 O lote a adquirido é composto por itens que envolvem tanto a aquisição dos equipamentos, **em regime de comodato**, quanto as licenças e os serviços relacionados a eles, como instalação e treinamento e licenciamento da solução.

1.6 O Lote 1, que compreende a solução integrada de Firewall Next Generation, objeto dessa licitação, deve conter, ao menos, os seguintes itens, com suas respectivas configurações mínimas:

ITEM	DESCRIÇÃO
1	APPLIANCE UTM de 10 Gbps de capacidade de firewall – alta disponibilidade por meio de equipamentos redundantes (2 - dois)
2	SOLUÇÃO DE GERENCIAMENTO WEB DE FIREWALL e ARMAZENAMENTO DE LOG POR 12 (DOZE) MESES EM NUVEM DO FABRICANTE COM AS LICENÇAS DE USO NECESSÁRIAS PARA ATENDIMENTO INTEGRAL DOS REQUISITOS PREVISTOS NESTE DOCUMENTO

3	SERVIÇO DE INSTALAÇÃO
4	TREINAMENTO PARA O SISTEMA DE FIREWALL UTM HANDS-ON
5	SERVIÇOS DE PRESTAÇÃO DE SUPORTE TÉCNICO REMOTO (NOC) 10X5 NA SOLUÇÃO COM HORAS ILIMITADAS E MONITORAMENTO 24X7.

1.7 **O detalhamento de todos os itens está descrito no Anexo II deste Termo de Referência.**

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 O SEPREV já possui a solução contratada através do Contrato nº 08/2020, atendendo perfeitamente às necessidades do Setor de Tecnologia da Informação.

2.2 Com o avanço tecnológico dos últimos anos, diversos serviços que antes eram executados muitas vezes de forma manual migraram para os meios digitais. Houve um grande ganho na agilidade e na prestação dos mais variados serviços que aderiram a essa modalidade. Tanto empresas quanto demais organizações e órgãos públicos investiram em equipamentos com o intuito de modernizar e melhorar a prestação de serviços aos seus respectivos públicos.

2.3 No entanto, na mesma proporção em que a tecnologia ganha espaço no mundo, muitos criminosos também veem a oportunidade de praticar crimes virtuais nesse novo contexto.

2.4 O Setor de Tecnologia da Informação – Departamento Administrativo tem se esforçado para proteger as informações de seus sistemas gerenciais, especialmente no que tange à proteção dos dados da população, cuja responsabilidade está atrelada à Lei Geral de Proteção de Dados Pessoais (LGPD).

2.5 Visando a constante melhoria e um maior nível de segurança para todos os usuários, o SEPREV reconhece a necessidade de adquirir um firewall, que é um dispositivo que atua na defesa da segurança de rede.

2.6 Ao contratar uma solução integrada de Firewall NEXT GENERATION, composta de hardware e software de segurança da informação do tipo UTM, destinada à proteção efetiva das informações contra-ataques cibernéticos, o SEPREV conseguirá garantir a interoperabilidade dos sistemas gerenciais e reforçar as medidas de proteção contra vazamentos de dados em conformidade com a LGPD (Lei Geral de Proteção de Dados), garantindo ainda maior proteção às informações e a todos os usuários.

2.7 Além de oferecer um nível maior de segurança à rede, um firewall de próxima geração (NGFW) possibilita a implementação de novos serviços, como, por exemplo, a análise do tráfego, que permite uma visualização detalhada da utilização da rede e das aplicações utilizadas, facilitando o processo de identificação de ameaças e permitindo a aplicação de políticas de segurança mais eficientes.

2.8 A efetivação da contratação permitiria ainda a identificação de usuários que utilizam a rede e o registro de conexões, informações extremamente importantes, seja para realizar a adequação ao Marco Civil da Internet ou para tratar incidentes de segurança.

2.9 Um firewall também oferece a possibilidade de gerar relatórios de forma rápida e detalhada sobre tudo o que acontece na rede, incluindo a rede wireless disponibilizada para a população em geral que visita a sede do escritório da autarquia para solicitação de serviços.

2.10 A adoção de uma solução de firewall possibilita à autarquia identificar e bloquear ameaças como vírus, trojans, spywares, ransomwares e outros tipos de malwares.

2.11 Todas essas características auxiliariam o Setor de Tecnologia da Informação no processo de reforçar a utilização das melhores práticas de segurança da informação, alinhando-se totalmente às exigências da Lei Geral de Proteção de Dados e ao Marco Civil da Internet.

2.12 Garantir essas camadas adicionais de proteção é essencial para proteger os computadores conectados à internet e os dados dos beneficiários do SEPREV.

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

3.1 A contratada será responsável pela disponibilização de solução integrada de Firewall NEXT GENERATION (NGFW) composta de Hardware e Software de segurança da informação do tipo UTM, destinado à proteção e segurança efetiva das informações contra-ataques cibernéticos, a fim de garantir a interoperatividade dos sistemas gerenciais do SEPREV e reforçar as medidas de proteção contra vazamentos de dados em relação à LGPD (Lei Geral de Proteção de Dados).

3.2 Uma vez que a contratação terá um custo inferior aos valores definidos no art. 75, II, da Lei nº 14.133/2021, o fornecedor será selecionado por meio de procedimento de dispensa de licitação.

3.3 A contratação será precedida pela divulgação de um aviso em sítio eletrônico oficial, pelo prazo de 3 (três) dias úteis, com a especificação do objeto pretendido e com a manifestação de interesse da Administração em obter propostas adicionais de eventuais interessados.

3.4 O lote a ser adquirido é composto por itens que envolvem tanto a aquisição dos equipamentos, em regime de comodato, quanto os serviços relacionados a eles, como instalação e treinamento e licenciamento da solução.

3.5 O item adquirido envolve a aquisição da solução completa, tanto o hardware, quanto os softwares e licenças necessárias para a sua efetiva implementação, incluindo também o serviço de suporte técnico.

3.6 Os produtos que compõe a Solução de Segurança devem todos ser produzidos pelo mesmo fabricante.

3.6.1 A empresa contratada deve informar na proposta comercial as marcas e modelos dos produtos ofertados.

3.7 A empresa contratada deverá realizar a instalação dos produtos contratados, deixando-os em perfeito estado de funcionamento.

3.8 O atraso no fornecimento da solução (NGFW) acarretará a aplicação das sanções previstas na Lei 14.133/2021 e suas correlatas, bem como as demais normas cabíveis, nos termos definidos no Edital.

3.9 Quaisquer outros equipamentos ou materiais necessários para a implantação da solução, nos moldes solicitados, devem ser fornecidos pela empresa contratada, sem qualquer ônus para o SEPREV.

3.10 Todas as despesas com o transporte, montagem, instalação, ou com quaisquer outros produtos ou serviços relacionados, incluindo a substituição em caso de defeito, mau funcionamento e obsolescência, correrão por conta da empresa contratada.

4. REQUISITOS DA CONTRATAÇÃO

4.1 Visando atender à demanda, é necessária a aquisição, em regime de comodato, de solução integrada de Firewall Next Generation para prevenção de ataques cibernéticos e proteção dos dados/informações dos computadores e servidores de arquivos do SEPREV, contemplando serviços de instalação, configuração e treinamento, bem como licenças de uso necessárias.

4.2 Considerando a complexidade da instalação dos equipamentos e estrutura da solução, a contratada deverá apresentar atestado/declaração de capacidade técnica, emitido por pessoas jurídicas de direito público ou privado, que comprove o fornecimento de equipamentos similares aos ofertados serviços de instalação, configuração e suporte técnico, devendo estar explicita a marca, modelos e as quantidades fornecidas;

4.3 A empresa contratada deve possuir um centro de operações de segurança, para atendimento com monitoramento dos serviços 24 horas por 7 dias semanais.

4.4 A contratada deve apresentar carta do fabricante quanto ao fornecimento, garantia e funcionalidade dos produtos ofertados.

4.5 A empresa contratada deve apresentar, ainda, atestado comprovando a existência de equipe técnica com pessoas capacitadas pelo fabricante em todas as soluções adquiridas.

4.5.1 O atestado deverá ser fornecido pelo fabricante.

4.6 A contratada deverá ter abrangência de atuação em todo o território nacional.

4.7 O fornecedor deverá apresentar preço fixo, em reais, equivalente ao de mercado.

4.7.1 Deverão estar inclusas todas as despesas sem quaisquer ônus para a autarquia, tais como encargos diretos e indiretos, impostos, taxas, transportes, fretes, seguros, mão-de-obra, deslocamento, carregamento, descarregamento, montagem, instalação, encargos sociais, trabalhistas, previdenciários, securitários e tributários ou outros decorrentes ou que venham a ser devidos em razão do mesmo.

5. DA EXECUÇÃO DO OBJETO

5.1 Condições de entrega:

5.1.1. Os serviços serão prestados dentro do melhor padrão de qualidade e confiabilidade, por meio de mão-de-obra técnica especializada, respeitadas as normas técnicas e legais a eles pertinentes.

5.1.2 O prazo para entrega, montagem e instalação da solução é de 30 (trinta) dias, contados da assinatura do contrato.

5.1.3 Caso não seja possível a execução na data estipulada, a empresa deverá comunicar as respectivas razões com, pelo menos, 15 (quinze) dias de antecedência, para que qualquer pedido de prorrogação de prazo seja analisado, ressalvadas as situações de caso fortuito e força maior.

5.1.4 Toda a logística é de responsabilidade da contratada, sem repasse ao SEPREV de qualquer custo adicional, além dos apresentados na proposta de fornecimento e transcritos no contrato.

5.1.5 O recebimento dos materiais ou serviços fornecidos ocorrerá da seguinte forma:

a) Recebimento provisório, após a finalização da montagem e instalação da solução, bem como do treinamento;

b) Recebimento definitivo, em até 5 (cinco) dias úteis contados do recebimento provisório, após a realização de testes que comprovem a operacionalidade do sistema e adequação do objeto aos termos contratados.

5.1.6 Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos ou corrigidos no prazo de até 05 (cinco) dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

5.1.7 O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do Contrato.

5.1.8 **Local e horário da prestação dos serviços:**

a) Os serviços serão prestados na sede do SEPREV, localizada à Rua dos Ipês, nº 125, Jardim Pompeia, Indaiatuba/SP.

b) Os serviços serão prestados nos seguintes horários: Os serviços, objeto deste TR, deverão ser executados pela CONTRATADA em horários previamente agendados junto ao SEPREV, conforme abaixo:

I) De segunda-feira a sexta-feira (exceto feriados e pontos facultativos), no horário de expediente do SEPREV, com acompanhamento de servidor do SEPREV.

6. DOS CRITÉRIOS DA ACEITABILIDADE DA PROPOSTA

6.1. A proposta deverá discriminar as características do objeto, condições de pagamento, execução e demais informações necessárias, que deverão estar em conformidade com este TR.

6.2. O prazo de validade da proposta deverá ser no mínimo de 60 (sessenta) dias, a contar da data estipulada para sua entrega.

6.3. O critério de julgamento das propostas será o de menor preço global.

6.4. O preço deverá ser fixo, em reais, equivalente ao de mercado.

6.5. Deverão estar incluídas, no preço dos serviços, todas as despesas sem quaisquer ônus para a administração pública, tais como frete, carga, descarga, tributos e quaisquer outros que incidam sobre a avença.

6.6. O valor da prestação dos serviços poderá ser reajustado pelo índice IPCA/IBGE, nos termos do art. 92, §4º, I, da Lei Federal n.º 14.133, de 1º de abril de 2021, mediante solicitação da CONTRATADA, após decorrido o prazo de 12 (doze) meses da assinatura do presente termo.

7. DOS REQUISITOS DE HABILITAÇÃO

7.1. A regularidade da empresa vencedora deverá ser demonstrada pelos seguintes documentos:

7.1.1. Prova de Inscrição no Cadastro Nacional de Pessoa Jurídica – Cartão CNPJ.

7.1.2. Prova de regularidade para com as Fazendas Federal, Estadual e Municipal.

7.1.2.1. A regularidade para com a Fazenda Federal deverá ser comprovada através da apresentação da Certidão Conjunta Negativa ou Positiva com Efeitos de Negativa de Débitos relativos a Tributos Federais e da Dívida Ativa da União, expedida pela Procuradoria Geral da Fazenda Nacional, incluída a regularidade junto à Seguridade Social (INSS).

7.1.2.2. A regularidade Estadual deverá ser comprovada através da apresentação da Certidão Negativa ou Positiva com Efeitos de Negativa de débitos relativos à Procuradoria Geral do Estado (Coordenadoria da Dívida Ativa), devendo compreender os débitos INSCRITOS NA DÍVIDA ATIVA.

7.1.2.3. A comprovação da regularidade fiscal municipal deverá ser apresentada através da certidão relativa a tributos mobiliários.

7.1.3. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS).

7.1.4. Certidão Negativa de Débitos Trabalhistas – CNDT, de acordo com a Lei 12440/11.

7.1.5. Certidão negativa correcional (ePAD, CGU-PJ, CEIS, CNEP e CEPIM).

7.2. As provas de regularidade deverão ser feitas por Certidão Negativa ou Certidão Positiva, com efeito de Negativa.

7.3. As certidões quando não tiveram expressamente informado o prazo de validade, terá seu vencimento considerado de até 180 (cento e oitenta) dias contados da data de sua emissão.

7.4. Os documentos mencionados acima deverão referir-se exclusivamente ao local do estabelecimento da interessada participante do presente processo, ressalvada a hipótese de centralização de recolhimento de tributos e contribuições pela matriz, que deverá ser comprovada por documento próprio, e estarem vigentes à época do envio da documentação.

7.5. Não serão aceitos protocolos referentes à solicitação feitas às repartições competentes quanto aos documentos acima mencionados, nem cópias ilegíveis sendo que as mesmas deverão ser apresentadas devidamente autenticadas.

8. MODELO DE GESTÃO DO CONTRATO

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

8.2. A execução do Contrato deverá ser acompanhada e fiscalizada por equipe indicada pelo SEPREV no ato da Contratação.

8.3. Competem ao Gestor e ao Fiscal as atribuições definidas no Decreto Federal nº 11.246, de 27 de outubro de 2022.

9. DO PAGAMENTO

9.1. O pagamento será realizado em parcelas mensais, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

9.2. O pagamento de cada parcela será efetuado no prazo máximo de até 15 (quinze) dias, contados da emissão de documento que ateste a efetiva entrega e realização de todos os produtos e serviços contratados ao longo do mês de referência, bem como o recebimento da Nota Fiscal/Fatura.

9.3. No caso de atraso pela contratante, os valores devidos serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária (Ou INPC).

9.4. Não será concedida antecipação de pagamento de créditos.

10. OBRIGAÇÕES DA CONTRATADA

10.1. A Contratada deve cumprir todas as obrigações constantes deste Termo de Referência, no edital e 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:

10.1.1. Entregar o objeto no prazo e nas condições estabelecidas;

10.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

10.1.3. Comunicar ao Contratante, no prazo máximo de 15 (quinze) dias que antecedem a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

10.1.4. Atender às determinações regulares emitidas pelo fiscal ou gestor do Contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

10.1.5. 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 verificar em vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

10.1.6. 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 contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

10.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do Contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica – (Cartão CNPJ); 2) Regularidade para com a Fazenda Federal - Certidão Conjunta Relativa aos Tributos Federais e à Dívida Ativa da União – (CND INSS); 3) Certidão Negativa de Débitos Trabalhistas – (CNDT) e 4) Certidão de Regularidade do FGTS – (CRF);

10.1.8. Manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação, ou para qualificação, na contratação direta.

10.1.9. Disponibilizar serviço de atendimento para registro de acionamento de possíveis falhas identificados na execução dos serviços, com atendimento ao usuário, realizado, pelo menos, no horário comercial (das 8h às 18h, de segunda a sexta-feira).

10.1.10. Disponibilizar os meios para se efetuar a abertura de pedidos de atendimento em garantia, via telefone ou internet.

10.1.11. Durante o período de garantia, sem qualquer ônus adicional para a autarquia, o atendimento compreenderá, quando necessário, a substituição dos materiais, peças, componentes e a mão-de-obra no reparo de defeitos de fabricação.

10.1.12. Manter sigilo sobre todas as informações inseridas na plataforma pelo Contratante a não ser os casos em que a quebra de sigilo seja determinada judicialmente, quando então deverá comunicar imediatamente a CONTRATANTE a fim de que esta possa exercer seu direito de defesa.

11. OBRIGAÇÕES DA CONTRATANTE

11.1. São obrigações da Contratante:

11.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o Termo de Referência e seus anexos;

11.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

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

11.1.4. Acompanhar e fiscalizar a execução do Contrato e o cumprimento das obrigações pelo Contratado;

11.1.5. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos neste Termo de Referência e no respectivo edital;

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

12. DO CONTRATO

12.1. A vigência do contrato será de 12 (doze) meses, podendo ser prorrogado, via termo aditivo, nas hipóteses legais a critério e interesse do CONTRATANTE, respeitada a vigência máxima decenal, conforme art. 107 da Lei Federal n.º 14.133, de 1º de abril de 2021. A minuta será elaborada posteriormente pelo Departamento Administrativo.

13. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

13.1. Na aplicação de penalidade/sanções serão observadas as disposições constantes na Lei nº 14.133, de 2021, que constam do respectivo edital, além das previstas nas legislações pertinentes.

14. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

14.1. Embora o objeto da contratação englobe uma solução completa, composta por vários elementos, somente um único item será adquirido. Dessa forma, a licitação será composta por um lote único.

14.2. O fornecedor será selecionado por meio da realização de procedimento de DISPENSA DE LICITAÇÃO, com fulcro no art. 75, II, da Lei nº 14.133/2021.

15. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

15.1. O custo estimado da contratação é de **R$ 29.132,40 (vinte e nove mil cento e trinta e dois reais e quarenta centavos).**

16. ADEQUAÇÃO ORÇAMENTÁRIA

16.1. As despesas decorrentes da contratação onerarão a dotação própria do orçamento vigente.

16.2. A presente contratação está prevista no PCA - Plano de Contratações Anual.

ANEXO II – ESPECIFICAÇÕES DO OBJETO

Para melhor dimensionamento do objeto licitado, de forma a propiciar o efetivo alcance dos objetivos pretendidos pelo SEPREV, os itens integrantes do objeto dessa licitação devem, obrigatoriamente, seguir as seguintes especificações:

ITEM 1: APPLIANCE UTM DE 10 GBPS DE CAPACIDADE DE FIREWALL

1.1 CARACTERÍSTICAS DO HARDWARE

1.1.1. Uma vez que a autarquia já possui rack, os equipamentos devem suportar sua instalação em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) do referido rack;

1.1.2. Para se adequar a estrutura da rede elétrica da sede do SEPREV, a solução deve dispor de fonte de alimentação interna ou externa com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

1.1.3. Possuir painel/led indicador on/off, disco e devices de rede;

1.1.4. Possuir throughput de no mínimo 6 Gbps para tráfego UDP, considerando pacotes de 64bytes;

1.1.5. Suportar no mínimo 700.000 (setecentos mil) conexões simultâneas;

1.1.6. Suportar no mínimo 35.000 (trinta e cinco mil) novas conexões por segundo;

1.1.7. Possuir throughput mínimo de 1,4 Gbps para tráfego IPS/IDS;

1.1.8. Possuir throughput mínimo de 6,5 Gbps para tráfego VPN IPSEC com criptografia (AES256-SHA256);

1.1.9. Possuir throughput mínimo de 900 Mbps para tráfego VPN SSL com criptografia (AES256);

1.1.10. Suportar no mínimo 200 (duzentos) usuários simultâneos de SSL VPN com licenciamento incluso;

1.1.11. Possuir throughput mínimo de 630 Mbps para tráfego SSL Inspection;

1.1.12. Suportar no mínimo 55.000 (cinquenta e cinco mil) conexões simultâneas com SSL Inspection;

1.1.13. Possuir throughput mínimo de 1 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

1.1.14. Possuir pelo menos 5 (cinco) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis;

1.1.15. Suportar a gestão de no mínimo 16 (dezesseis) APs (access point) do mesmo fabricante em modo Bridge ou de comutação local, e no mínimo 8 (oito) access points em modo túnel ;

1.1.16. Suportar no mínimo 10 (dez) domínios virtuais;

1.1.17. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

1.1.18. Possuir no mínimo 1 (uma) porta USB para conexão de dispositivos externos;

1.1.19. Possuir no mínimo 1 (uma) porta Console RJ45 isolada

1.1.20. Fornecimento de 2 (dois) equipamentos conectados e configurados em cluster de firewall redundantes para alta disponibilidade, minimizando o tempo de inatividade em caso de falha.

1.1.21. Modelo de referência: Fortinet 60F

ITEM 2: ESPECIFICAÇÃO GERAL DE SOFTWARE NGFW PARA O ITEM 1 DESTE ANEXO

2.1 FUNÇÕES BÁSICAS

2.1.1 Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;

2.1.2 VPN SSL, VPN IPSec (Client-to-site e Site-to-site);

2.1.3 Controle de Aplicações;

2.1.4 Proxy Web e Filtro de Conteúdo Web (Web Filtering);

2.1.5 Detecção e prevenção de intrusos – IPS;

2.1.6 Qualidade de serviço – QOS;

2.1.7 Anti-Malware/Sandbox;

2.1.8 SD-WAN;

2.1.9 Gerenciamento centralizado para Firewall, APs (Access Point) e Switch do mesmo fabricante;

2.1.10 Cluster.

2.2 CARACTERÍSTICAS GERAIS PARA O EQUIPAMENTO DE NGFW

2.2.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização para os equipamentos dos itens 1, 2, 3, 4 e 5 deste Anexo;

2.2.2 A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);

2.2.3 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

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

2.2.5 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

2.2.6 Os dispositivos de proteção de rede devem possuir suporte a Vlans;

2.2.7 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

2.2.8 Deve suportar BGP, OSPF, RIP e roteamento estático;

2.2.9 Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

2.2.10 Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

2.2.11 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

2.2.12 Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;

2.2.13 Deve suportar NAT dinâmico (Many-to-Many);

2.2.14 Deve suportar NAT estático (1-to-1);

2.2.15 Deve suportar NAT estático bidirecional 1-to-1;

2.2.16 Deve suportar Tradução de porta (PAT);

2.2.17 Deve suportar NAT de Origem;

2.2.18 Deve suportar NAT de Destino;

2.2.19 Deve suportar NAT de Origem e NAT de Destino simultaneamente;

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

2.2.21 Deve suportar NAT64;

2.2.22 Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

2.2.23 Enviar log para sistemas de monitoração externos;

2.2.24 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

2.2.25 Proteção anti-spoofing;

2.2.26 Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

2.2.27 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

2.2.28 A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;

2.2.29 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

2.2.30 Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound);

2.2.31 A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

2.2.32 Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

2.2.33 Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-ofsale;

2.2.34 A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

2.2.35 Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

2.2.36 Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de compliance na VPN;

2.3 POLÍTICAS

2.3.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização para os equipamentos dos itens 1, 2, 3, 4 e 5 deste Anexo;

2.3.2 Deverá suportar controles por zonas de segurança;

2.3.3 Deverá suportar controles de políticas por porta e protocolo;

2.3.4 Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

2.3.5 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

2.3.6 Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

2.3.7 Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

2.3.8 Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

2.3.9 Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

2.3.10 Suporte a objetos e regras IPV6;

2.3.11 Suporte a objetos e regras multicast;

2.3.12 Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

2.4 CONTROLE DE APLICAÇÕES

2.4.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização pelo período total de, no mínimo, 60 meses para os equipamentos dos itens 1 e 2 deste Anexo;

2.4.2 As características descritas abaixo devem ser totalmente suportadas, podendo ser, a qualquer momento da vida útil dos equipamentos, licenciadas para utilização efetiva para os equipamentos dos itens 3, 4 e 5 deste Anexo;

2.4.3 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.4.4 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

2.4.5 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

2.4.6 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

2.4.7 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

2.4.8 Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

2.4.9 Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

2.4.10 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

2.4.11 Identificar o uso de táticas evasivas via comunicações criptografadas;

2.4.12 Atualizar a base de assinaturas de aplicações automaticamente;

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

2.4.14 Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

2.4.15 Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

2.4.16 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

2.4.17 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

2.4.18 Deve alertar o usuário quando uma aplicação for bloqueada;

2.4.19 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

2.4.20 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

2.4.21 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

2.4.22 Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

2.4.23 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

2.4.24 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;

2.4.25 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

2.4.26 Deve permitir forçar o uso de portas específicas para determinadas aplicações;

2.4.27 Deve permitir o filtro de vídeos que podem ser visualizados no YouTube;

2.5 PREVENÇÃO DE AMEAÇAS

2.5.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização pelo período total de, no mínimo, 60 meses para os equipamentos dos itens 1 e 2 deste Anexo;

2.5.2 As características descritas abaixo devem ser totalmente suportadas, podendo ser, a qualquer momento da vida útil dos equipamentos, licenciadas para utilização efetiva para os equipamentos dos itens 3, 4 e 5 deste Anexo;

2.5.3 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

2.5.4 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e AntiSpyware);

2.5.5 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

2.5.6 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

2.5.7 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

2.5.8 Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

2.5.9 Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

2.5.10 Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

2.5.11 Deve permitir o bloqueio de vulnerabilidades;

2.5.12 Deve permitir o bloqueio de exploits conhecidos;

2.5.13 Deve incluir proteção contra-ataques de negação de serviços;

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

2.5.15 Detectar e bloquear a origem de portscans;

2.5.16 Bloquear ataques efetuados por worms conhecidos;

2.5.17 Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

2.5.18 Possuir assinaturas para bloqueio de ataques de buffer overflow;

2.5.19 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

2.5.20 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

2.5.21 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, SSH, FTP, SMB, SMTP e POP3;

2.5.22 Identificar e bloquear comunicação com botnets;

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

2.5.24 Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

2.5.25 Os eventos devem identificar o país de onde partiu a ameaça;

2.5.26 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

2.5.27 Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

2.5.28 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

2.5.29 Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

2.5.30 Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

2.5.31 A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

2.6 FILTRO DE URLs

2.6.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização pelo período total de, no mínimo, 60 meses para os equipamentos dos itens 1 e 2 deste Anexo;

2.6.2 As características descritas abaixo devem ser totalmente suportadas, podendo ser, a qualquer momento da vida útil dos equipamentos, licenciadas para utilização efetiva para os equipamentos dos itens 3, 4 e 5 deste Anexo;

2.6.3 Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

2.6.4 Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

2.6.5 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;

2.6.6 A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

2.6.7 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

2.6.8 Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

2.6.9 Possuir pelo menos 60 categorias de URLs;

2.6.10 Deve possuir a função de exclusão de URLs do bloqueio;

2.6.11 Permitir a customização de página de bloqueio;

2.6.12 Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

2.6.13 Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

2.6.14 Os requisitos de filtro de URL descritos acima aplicam-se apenas ao firewall das pontas remotas;

2.7 IDENTIFICAÇÃO DE USUÁRIOS

2.7.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização para os equipamentos dos itens 1, 2, 3, 4 e 5 deste Anexo;

2.7.2 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Edirectory e base de dados local;

2.7.3 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.7.4 Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

2.7.5 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

2.7.6 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.7.7 Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

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

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

2.7.10 Deve suportar o envio e recebimento de credenciais via RADIUS;

2.8 FILTRO DE DADOS

2.8.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização pelo período total de, no mínimo, 60 meses para os equipamentos dos itens 1 e 2 deste Anexo;

2.8.2 As características descritas abaixo devem ser totalmente suportadas, podendo ser, a qualquer momento da vida útil dos equipamentos, licenciadas para utilização efetiva para os equipamentos dos itens 3, 4 e 5 deste Anexo;

2.8.3 Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

2.8.4 Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

2.8.5 Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

2.8.6 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

2.9 GEOLOCALIZAÇÃO

2.9.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização para os equipamentos dos itens 1, 2, 3, 4 e 5 deste Anexo;

2.9.2 Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

2.9.3 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

2.10 VPN CLIENT-TO-SITE

2.10.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização para os equipamentos dos itens 1, 2, 3, 4 e 5 deste Anexo;

2.10.2 Suportar IPSec VPN;

2.10.3 Suportar SSL VPN;

2.10.4 A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

2.10.5 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

2.10.6 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

2.10.7 Atribuição de DNS nos clientes remotos de VPN, inclusive com DNS split tunnel;

2.10.8 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

2.10.9 Suportar autenticação via AD/LDAP, certificado e base de usuários local;

2.10.10 Suportar leitura e verificação de CRL (certificate revocation list);

2.10.11 Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

2.10.12 A VPN SSL deve permitir aos usuários remotos a troca de senha no Active Directory;

2.10.13 O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.14 e superior).

2.11 RECURSOS GERAIS DE SD-WAN

2.11.1 As características descritas abaixo devem ser totalmente suportadas e devidamente licenciadas para implementação e utilização para os equipamentos dos itens 1, 2, 3, 4 e 5 deste Anexo;

2.11.2 A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

2.11.3 Deve ser possível criar políticas que definam os seguintes critérios para match:

2.11.4 Endereços de origem;

2.11.5 Grupos de usuários;

2.11.6 Endereços de destino;

2.11.7 DSCP;

2.11.8 Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

2.11.9 A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

2.11.10 O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

2.11.11 O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;

2.11.12 Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

2.11.13 A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;

2.11.14 Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

2.11.15 A solução deve permitir a definição do roteamento para cada aplicação;

2.11.16 Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

2.11.17 Deve possibilitar a definição do link de saída para uma aplicação específica;

2.11.18 Deve implementar balanceamento de link por hash do IP de origem;

2.11.19 Deve implementar balanceamento de link por hash do IP de origem e destino;

2.11.20 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

2.11.21 Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

2.11.22 A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

2.11.23 Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

2.11.24 Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

2.11.25 Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

2.11.26 A solução de SD-WAN deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP;

2.11.27 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

2.11.28 Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

2.11.29 O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

2.11.30 O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;

2.11.31 Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

2.11.32 O QoS deve possibilitar a definição de fila de prioridade;

2.11.33 Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

2.11.34 A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;

2.11.35 Deve possibilitar a definição de bandas distintas para download e upload;

2.11.36 A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

2.11.37 A solução de SD-WAN deve suportar IPv6;

2.11.38 Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

2.11.39 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

2.11.40 O SD-WAN deverá possuir serviço de Firewall Stateful;

2.11.41 A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

2.11.42 A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

2.11.43 Deve ser capaz de bloquear acesso às aplicações;

2.11.44 Deve suportar NAT dinâmico bem como NAT de saída;

2.11.45 Deve suportar balanceamento de tráfego por sessão e pacote;

2.11.46 Suportar VPN IPSec Site-to-Site;

2.11.47 A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

2.11.48 A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

2.11.49 A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14,Group 15 até 21 e Group 27 até 32;

2.11.50 A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

2.11.51 A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

2.11.52 Deve suportar o uso de DDNS, para casos onde uma ou ambas as pontas possuam IPs dinâmicos;

2.11.53 Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;

2.11.54 Deve possuir suporte e estar licenciamento para uso de VRFs;

2.11.55 A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance;

2.12 SD-WAN

2.12.1 O fornecedor deve considerar recursos de gestão centralizada para as soluções NGFW e SDWAN;

2.12.2 Devem ser do mesmo fornecedor das soluções ofertadas, suportando nativamente todos os recursos listados;

2.12.3 Pode ser ofertado em VM, desde que compatível com VMware ESXI 5.5 e acima, Hyper-V 2008 e acima e KVM;

2.12.4 Pode ser ofertado em hardware, desde que em appliance do próprio fabricante;

2.12.5 Deve considerar o volume de equipamentos ofertados, considerando todo o licenciamento necessário para a correta gestão dos elementos de rede;

2.12.6 Deve ter a capacidade mínima e estar licenciado para:

2.12.7 Processar 06 GB de log por dia;.

2.12.8 Mínimo de 3.5 TB de capacidade de armazenamento;

2.13 CARACTERÍSTICAS DE GERÊNCIA CENTRALIZADA DE NGFW

2.13.1 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

2.13.2 O sistema deverá suportar contas de usuário/senha estáticas;

2.13.3 Permitir acesso concorrente de administradores;

2.13.4 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

2.13.5 O sistema deverá suportar o método de autenticação externo usuário/conta do servidor Radius;

2.13.6 A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;

2.13.7 Essas comunicações deverão ser protegidas e criptografadas;

2.13.8 Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento;

2.13.9 Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;

2.13.10 A console de Gerência deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN;

2.13.11 Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência.

2.13.12 Os resultados de desempenho de link e aplicativo deverão ser visualizados em forma de gráfico a partir da GUI de Gerência SD-WAN;

2.13.13 O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;

2.13.14 O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

2.13.15 O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

2.13.16 Permitir localizar quais regras um objeto está sendo utilizado;

2.13.17 Permitir criação de regras que fiquem ativas em horário definido;

2.13.18 A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;

2.13.19 Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

2.13.20 Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas as mesmas somente sejam aplicadas após aprovação de outro administrador;

2.13.21 Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;

2.13.22 Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;

2.13.23 Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;

2.13.24 Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;

2.13.25 Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

2.13.26 Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;

2.13.27 Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;

2.13.28 Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;

2.13.29 Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;

2.13.30 Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;

2.13.31 Permitir criar regras anti DDoS de forma centralizada;

2.13.32 Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

2.13.33 Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;

2.13.34 Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;

2.13.35 Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes, etc.;

2.13.36 Deve possuir recursos de playbook que, por meio de integrações com soluções de firewall, endpoint, email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;

2.13.37 Deve oferecer portal personalizado para gerenciamento de dispositivos, APs, políticas e objetos, junto com painéis, relatórios e visualizações personalizadas para atualizações de segurança abrangentes, análises em tempo real e respostas exclusivas às suas necessidades;

2.13.38 Deve permitir a correlação de eventos, provendo dashboards diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

2.13.39 O portal deve permitir uma visão geral do tráfego de rede e da postura de segurança, incluindo widgets intuitivos com informações como principais países, principais ameaças, principais origens de tráfego, principais destinos, principais aplicativos e hits de políticas, bem como gráficos para mostrar logins de administrador, eventos do sistema, e uso de recursos;

2.13.40 O portal deve suportar a sua configuração possibilite seu uso via multi-tenant, ou seja, com a possibilidade de se criarem vários portais de acesso independentes entre si para fins de administração distribuída;

2.13.41 Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

2.13.42 Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

2.13.43 A gerência centralizada deve vir acompanhada com solução de visualização de logs e geração de relatórios. Esta solução pode ser disponibilizada no mesmo equipamento de gerenciamento centralizado, ou fornecido em equipamento externo do mesmo fabricante;

2.13.44 Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

2.13.45 Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

2.13.46 Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

2.13.47 Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

2.13.48 Deve possuir mecanismos de remoção automática para logs antigos;

2.13.49 Permitir importação e exportação de relatórios

2.13.50 Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

2.13.51 Deve permitir exportar os logs no formato CSV;

2.13.52 Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

2.13.53 Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

2.13.54 A solução deve ter relatórios predefinidos;

2.13.55 Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

2.13.56 Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

2.13.57 Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

2.13.58 Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

2.13.59 Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

2.13.60 Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

2.13.61 Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

2.13.62 Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

2.13.63 Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

2.13.64 Permitir o envio por e-mail relatórios automaticamente;

2.13.65 Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;

2.13.66 Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

2.13.67 Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

2.13.68 Deve permitir o uso de filtros nos relatórios;

2.13.69 Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

2.13.70 Permitir especificar o idioma dos relatórios criados;

2.13.71 Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

2.13.72 Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

2.13.73 Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

2.13.74 Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

2.13.75 Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

2.13.76 Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

2.13.77 Deve permitir visualizar em tempo real os logs recebidos;

2.13.78 Deve permitir o encaminhamento de log no formato syslog;

2.13.79 Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

2.13.80 Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

2.13.81 Deve permitir gerar alertas de eventos a partir de logs recebidos.

ITEM 3: SERVIÇO DE INSTALAÇÃO

3.1 Para as soluções ofertadas, a contratada deverá oferecer um valor total para a instalação e customização inicial dos dispositivos adquiridos;

3.2 Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;

3.3 A instalação deve ser feita na sede do SEPREV, por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;

3.4 Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada;

3.5 As configurações, regras e políticas implementadas nos dispositivos atualmente instalados, deverão ser transferidas para os novos dispositivos, a cargo da CONTRATADA.

ITEM 4: TREINAMENTO PARA O SISTEMA DE FIREWALL UTM

4.1 Deverá ser fornecido treinamento para a solução de firewall adquirida (hardware ou software) para a equipe do cliente HandsOn;

4.2 Carga Horária mínima de 8 (oito) horas;

4.3 O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação;

4.4 O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;

4.5 Este treinamento será realizado em ambiente interno da CONTRATANTE.

4.6 Os cursos deverão ser realizados em horários e data a serem acordados pela CONTRATADA e CONTRATANTE, devendo respeitar o horário de expediente do SEPREV;

ITEM 5: SERVIÇOS DE PRESTAÇÃO DE SUPORTE TÉCNICO REMOTO 8X5

5.1 Serviço de suporte remoto para a solução contratada, no horário 8x5 (Segunda a sexta-feira das 08:00 às 18:00, exceto feriados), pelo tempo de contrato, com as seguintes características:

5.2 A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;

5.3 A contratada deverá iniciar o atendimento de suporte em no máximo 2 horas úteis após a abertura do chamado. Se o funcionamento da solução estiver totalmente interrompido, o prazo para resolução será de no máximo 4 (quatro) horas corridas.

5.4 A contratada deverá fornecer atestado comprovando a existência de equipe técnica de no mínimo 3 pessoas capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante;

5.5 A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações:

5.5.1 Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;

5.5.2 A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno;

5.5.3 Competirá à contratada promover a análise de viabilidade quanto a instalação de novas versões disponibilizadas dos produtos, e, sendo favorável, implementar a atualização em horário previamente acordado com o SEPREV.

5.5.4 Fazem parte dos serviços a serem executados pela CONTRATADA a prestação de serviços de suporte para esclarecimento de dúvidas e apoio nas configurações da solução ofertada.

ANEXO III - MINUTA CONTRATUAL

TERMO DE CONTRATO PARA PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI FAZEM O SEPREV – SERVIÇO DE PREVIDÊNCIA E ASSISTÊNCIA À SAÚDE DOS SERVIDORES MUNICIPAIS DE INDAIATUBA E [inserir nome da contratada].

CONTRATO Nº: __/____
PROC. ADMINISTRATIVO Nº: 1.520/2024
DATA: __/__/____
PRAZO: 12 (DOZE) MESES
FUNDAMENTO: ART. 75, INCISO II, DA LEI Nº 14.133/2021

Pelo presente instrumento, de um lado o **SEPREV – SERVIÇO DE PREVIDÊNCIA E ASSISTÊNCIA À SAÚDE DOS SERVIDORES MUNICIPAIS DE INDAIATUBA**, com sede na Rua dos Ipês, nº 125, Jardim Pompéia, CEP 13.345-060, município de Indaiatuba, estado de São Paulo, e-mail: contato@seprev.sp.gov.br, inscrito no CNPJ nº 68.004.118/0001-21, neste ato representado por seu Superintendente, **ANTONIO CORRÊA**, CPF sob o nº 107.837.418-04, ora chamado simplesmente **CONTRATANTE ou SEPREV**; e de outro lado a empresa, **[inserir nome da contratada]**, situada na Rua _____, nº ___, Bairro _____, Município de _____, Estado de _____, CEP: _____-___, e-mail: _____, inscrita no CNPJ nº __.___.___/____-__, neste ato representada por seu (sua) representante legal, **[inserir nome do representante legal]**, CPF nº ___.___.___-__, doravante designada simplesmente **CONTRATADA**, decorrente do Processo nº 1.442/2024, realizada nos termos da Lei Federal n.º 14.133/2021, com suas alterações subsequentes e demais normas complementares, mediante as cláusulas e condições a seguir estabelecidas e que reciprocamente outorgam e aceitam.

CLAUSULA 1ª – DO OBJETO

1.1. O objeto do presente contrato consiste na contratação de solução integrada de Firewall Next Generation, com sistema redundante em alta disponibilidade, contemplando o fornecimento de equipamentos e de licenças, para prevenção de ataques cibernéticos e proteção dos dados e informações dos computadores e servidores de arquivos do SEPREV, por um período de 12 (doze) meses, de acordo com as especificações abaixo:

1.1.1. A execução dos serviços ocorrerá de acordo com o detalhamento constante no Termo de Referência (Anexo I) do Processo nº 1.520/2024 e conforme a proposta de preços apresentada pela CONTRATADA. Esses documentos, independentemente de transcrição ou anexação, são partes integrantes do presente instrumento.

1.1.2. A CONTRATADA compromete-se a cumprir integralmente o objeto deste contrato, conforme estabelecido com base no art. 72 em conjunto com o art. 75, II, da Lei Federal n.º 14.133, de 1º de abril de 2021.

CLÁUSULA 2ª - DA EXECUÇÃO DO CONTRATO

2.1. O objeto ora contratado deverá ser executado com estrita observância ao que dispõe a Proposta da CONTRATADA, aos termos deste contrato e aos demais elementos constantes do Processo nº 1.520/2024, que integram o presente instrumento, independentemente de transcrição ou anexação.

2.2. O CONTRATANTE poderá, em qualquer ocasião, exercer a mais ampla fiscalização dos serviços, reservando-se o direito de rejeitá-los, a seu critério, quando não forem considerados satisfatórios.

2.3. A fiscalização, por parte do CONTRATANTE, não eximirá a CONTRATADA das responsabilidades previstas na legislação civil e por danos a que direta e comprovadamente vier causar ao CONTRATANTE ou a terceiros, seja por seus atos, de seus funcionários ou prepostos, decorrentes comprovadamente de sua culpa ou dolo na execução do contrato, nos termos da Cláusula 4ª.

2.4. Havendo qualquer falha comprovada na execução do contrato ou desacordo com as normas, a CONTRATADA será previamente notificada para que os regularize no prazo de 05 (cinco) dias, sob pena de aplicação das penalidades previstas neste contrato.

CLÁUSULA 3ª - DAS OBRIGAÇÕES DAS PARTES

3.1. Caberá à CONTRATADA observar escrupulosamente as boas práticas dos serviços, respeitando com fidelidade as orientações contidas no Anexo I - Termo de Referência, bem como as leis, regulamentos e posturas federais, estaduais e municipais pertinentes ao objeto deste instrumento. A CONTRATADA deverá cumprir imediatamente as intimações e exigências das respectivas autoridades, além de:

3.1.1. Caberá à CONTRATADA o pagamento de todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir direta ou indiretamente sobre o objeto deste instrumento.

3.1.2. São de responsabilidade da CONTRATADA os encargos tributários e trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas referentes aos serviços executados por seus empregados, decorrentes da presente avença, isentando o CONTRATANTE de quaisquer responsabilidades, inclusive por danos contra terceiros.

3.1.3. A CONTRATADA fica obrigada a manter, durante a vigência do contrato, as condições de participação, habilitação e qualificação exigidas para a contratação.

3.2. O CONTRATANTE obriga-se a propiciar todas as facilidades indispensáveis à boa realização do objeto deste instrumento.

3.3. O CONTRATANTE obriga-se, ainda, a efetuar pontualmente os pagamentos referentes aos serviços efetuados pela CONTRATADA.

CLÁUSULA 4ª - DA RESPONSABILIDADE PELO RESSARCIMENTO DE DANOS

4.1. A CONTRATADA se responsabilizará por danos causados por seus funcionários e/ou terceiros na prestação de serviços, objeto deste contrato, garantida ampla defesa, exceto quando comprovada a culpa única e exclusiva do CONTRATANTE.

4.1.1. Na hipótese do CONTRATANTE ser demandado por qualquer pessoa em razão de danos provocados por culpa da CONTRATADA ou seus prepostos, após devidamente apurado e comprovado, esta, obriga-se a ressarcir o CONTRATANTE e ao terceiro prejudicado, regressivamente, tudo o quanto tiver de dispender incluindo eventuais indenizações, custas ou despesas, judiciais ou extrajudiciais, honorários advocatícios, desde que o CONTRATANTE comunique imediatamente à

CONTRATADA ao receber qualquer notificação, citação ou intimação, para que a mesma possa apresentar defesa.

CLÁUSULA 5ª – DA SEGURANÇA DA INFORMAÇÃO E DA PROTEÇÃO DE DADOS PESSOAIS

5.1. No decorrer de quaisquer atividades relacionadas à execução deste contrato, as Partes comprometem-se a seguir rigorosamente o regime legal da proteção de dados pessoais, conforme estabelecido pela Lei Federal nº 13.709, de 14 de agosto de 2018, e demais normas vigentes relacionadas, e as diretrizes estabelecidas na Política de Segurança da Informação do SEPREV, aprovada pela Resolução nº 327, de 12 de dezembro de 2019.

CLÁUSULA 6ª – DA VIGÊNCIA E PRAZO

6.1. A vigência do presente contrato será de 12 (doze) meses, vigorando no período de __ de _____ de ____ a __ de _____ de ____, podendo ser prorrogado, mediante termo aditivo, nas hipóteses legais, a critério e interesse do CONTRATANTE, respeitada a vigência máxima decenal, conforme estabelecido no art. 107 da Lei Federal n.º 14.133, de 1º de abril de 2021.

CLÁUSULA 7ª – DA REMUNERAÇÃO E PAGAMENTO

7.1. Pela entrega do objeto da prestação de serviços, conforme especificado na cláusula 1ª e no Termo de Referência, o CONTRATANTE compromete-se a remunerar a CONTRATADA o montante de R$ ( ), dividido em 12 (doze) parcelas mensais de R$ ( ) cada.

7.1.1. O pagamento será efetuado pelo SEPREV mediante a apresentação de documento fiscal à gestor(a) do contrato, no prazo de até 15 (quinze) dias. O(a) gestor(a) do contrato é responsável por atestar os serviços prestados e liberar o pagamento. Eventuais ajustes e não conformidades devem ser resolvidos pela Contratada junto ao(à) gestor(a).

7.1.2. O pagamento em atraso ensejará a incidência de correção monetária “pro rata” pela variação do INPC/IBGE, juros, também “pro rata dia” de 1% (um por cento) ao mês e multa moratória de 2% (dois por cento) após o 10º (décimo) dia.

7.2. Os valores descritos nesta cláusula poderão ser reajustados pelo índice IPCA/IBGE, nos termos do art. 92, §4º, I, da Lei Federal n.º 14.133, de 1º de abril de 2021.

7.3. Nos preços indicados estão incluídas, além dos lucros, todas as despesas de custos, benefícios, tributos e quaisquer outras despesas direta ou indiretamente relacionadas com a execução do objeto deste instrumento, cuja composição dos custos, poderá ser solicitada pelo CONTRATANTE.

7.4. Caso ocorram erros na Nota Fiscal, a gestor(a) do contrato comunicará imediatamente a CONTRATADA para que efetue as devidas correções. O prazo de pagamento será contado a partir da data de apresentação da Nota Fiscal sem erros.

7.5. Nenhum pagamento antecipado será efetuado à CONTRATADA, ou enquanto pendente de liquidação qualquer obrigação financeira que lhe foi imposta, em virtude de penalidade ou inadimplência, a qual poderá ser compensada com o pagamento pendente, sem que isso gere direito a acréscimos de qualquer natureza.

7.6. O contrato poderá ser alterado, com as devidas justificativas para restabelecer a relação que as Partes pactuaram inicialmente entre os encargos da CONTRATADO e a retribuição da Administração para a justa remuneração do objeto contratado, objetivando a manutenção de equilíbrio econômico financeiro inicial do contrato, na hipótese de sobrevirem fatos imprevisíveis, ou previsíveis, porém, de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

7.7. Quaisquer tributos ou encargos legais criados, alterados ou extintos, bem como a superveniência de disposições legais, quando ocorridas após a data de apresentação da Proposta, de comprovada repercussão nos preços contratados, poderão implicar a revisão destes para mais ou menos, conforme o caso.

7.8. Na hipótese de a CONTRATADA solicitar alteração de preço, esta terá que justificar o pedido, através de planilha detalhada de custos, acompanhada de documentos que comprovem a procedência do pedido.

CLÁUSULA 8ª – DO SUPORTE LEGAL E ORÇAMENTÁRIO

8.1. O valor total da presente avença para __ (_____) _____ é de R$ _____,__ (_____). As despesas decorrentes da execução deste contrato serão suportadas pela dotação orçamentária vigente, codificada pelo nº **[especificar]**, cujo valor será informado na Nota de Empenho, emitida pelo Departamento Financeiro.

8.2. O presente contrato é firmado através do Processo n.º 1.520/2024 com fundamento no art. 72 em conjunto com o art. 75, II da Lei Federal n.º 14.133, de 1º de abril de 2021, pelas quais se regerá, sendo que a Proposta da CONTRATADA fica fazendo parte integrante deste instrumento.

CLÁUSULA 9ª – DA FISCALIZAÇÃO E GESTÃO

9.1. A execução deste contrato será acompanhada e fiscalizada pelos servidores designados abaixo, competindo-lhes as atribuições definidas no Decreto Federal nº 11.246, de 27 de outubro de 2022:

a) Gestor(a): _____

b) Fiscal Técnico e Administrativo: _____

9.2. O preposto da CONTRATADA será, _____, CPF nº _____, e-mail:_____, para fiscalizar a execução deste contrato, prestar toda assistência e orientação que se fizerem necessárias, conforme art. 118 da Lei Federal n.º 14.133, de 1º de abril de 2021.

CLÁUSULA 10ª – DAS PENALIDADES E RESCISÃO

10.1. Em caso de inexecução total ou parcial do contrato, garantida notificação para prévia defesa, a CONTRATADA poderá incorrer em sanção, de acordo com a falta cometida, conforme critérios do art. 156, §1º, da Lei n.º 14.133/2021.

10.1.1. A recusa injustificada do adjudicatário em assinar o presente instrumento, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido pelo SEPREV, caracterizará o descumprimento total da obrigação assumida, sujeitando-o às seguintes penalidades:

I - Multa de 10% (dez por cento) sobre o valor da obrigação não cumprida; ou

II - Pagamento correspondente à diferença de preço decorrente de nova licitação para o mesmo fim.

10.1.2. Para os demais casos, as sanções podem ser:

I - Advertência;

II - Multa de 2% (dois por cento) sobre o valor da obrigação não cumprida; e

III - Cancelamento do instrumento e suspensão temporária de participação em licitação e impedimento de contratar com o SEPREV, pelo prazo de até 02 (dois) anos.

10.2. As sanções serão independentes entre si, podendo ser aplicadas isolada ou cumulativamente com a multa, conforme art. 156, §7º, da Lei n.º 14.133/2021.

10.3. Se o valor da multa ou indenização devida não for recolhida dentro do prazo de 30 (trinta) dias corridos contados a partir da data do recebimento da notificação com a decisão após a defesa prévia da CONTRATADA, a inadimplência da empresa será inscrita em Dívida Ativa e executada judicialmente.

10.4. As penalidades previstas nesta Cláusula têm caráter de sanção administrativa, e, consequentemente, a sua aplicação não exime a empresa detentora do presente instrumento da reparação das eventuais e comprovadas perdas e danos que seu ato punível venha acarretar ao SEPREV, nos termos da Cláusula 4ª.

10.5. Após a aplicação de quaisquer das penalidades acima previstas, realizar-se-à comunicação escrita à empresa, e a publicação na Imprensa Oficial do Município ou Diário Oficial do Estado (excluídas as penalidades de advertência e multa de mora), constando o fundamento legal da punição e que o fato será registrado no cadastro correspondente, inclusive junto ao Tribunal de Contas do Estado de São Paulo.

10.6. A aplicação de multas que, em conjunto, e dentro de um mesmo anuênio contratual, ultrapasse o equivalente a 30% (trinta por cento) do valor total do presente contrato, será causa de rescisão do contrato, unilateralmente, pelo SEPREV, nos termos da legislação aplicável.

10.7. Nenhuma sanção será aplicada sem o devido processo administrativo, que prevê defesa prévia do interessado e recurso nos prazos definidos em lei, sendo-lhe franqueado vista ao processo.

10.8. Aquele que firmar declaração falsa, inclusive documentos, ou que dela tenha conhecimento, ficará sujeito às penas da Lei de Licitações, sem prejuízo da responsabilidade criminal cabível.

10.9. A extinção do contrato poderá ser:

I - Determinada por ato unilateral e escrito do SEPREV, exceto no caso de descumprimento decorrente de sua própria conduta;

II - Consensual, por acordo entre as Partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse do SEPREV;

III - Determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

10.9.1. A extinção determinada por ato unilateral do SEPREV e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.

10.9.2. Quando a extinção decorrer de culpa exclusiva do SEPREV, a CONTRATADA será ressarcida pelos prejuízos regularmente comprovados que houver sofrido e terá direito a:

I - Devolução da garantia, se for o caso;

II - Pagamentos devidos pela execução do contrato até a data de extinção; e

III - Pagamento do custo da desmobilização, se for o caso.

10.10. Poderão constituir motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as situações descritas no art. 137 da Lei n.º 14.133/2021.

10.11. A CONTRATADA terá direito à extinção do contrato nas seguintes hipóteses:

I - Supressão, por parte do SEPREV, do objeto do contrato que acarrete modificação do valor inicial do contrato além do limite permitido no art. 125 da Lei n.º 14.133/2021;

II - Suspensão de execução do contrato, por ordem escrita do SEPREV, por prazo superior a 3 (três) meses;

III - Repetidas suspensões que totalizem 90 (noventa) dias úteis, independentemente do pagamento obrigatório de indenização pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas;

IV - Atraso superior a 2 (dois) meses, contado da emissão da Nota Fiscal, dos pagamentos ou de parcelas de pagamentos devidos pelo SEPREV no âmbito deste contrato;

V - Não liberação pela Administração, nos prazos contratuais, de área, local ou objeto, para execução do objeto do contrato.

10.12. Fazem parte desta Cláusula as demais previsões constantes no CAPÍTULO VIII – DAS HIPÓTESES DE EXTINÇÃO DOS CONTRATOS da Lei n.º 14.133/2021, naquilo que for aplicável.

CLÁUSULA 11ª – DO CÓDIGO DE ÉTICA E DAS DECLARAÇÕES E GARANTIAS DE ANTICORRUPÇÃO

11.1. As Partes declaram neste ato, ciência e compromisso de respeitarem o Código de Ética do SEPREV, aprovado pela Resolução nº 302, de 30 de agosto de 2018, e de se absterem de qualquer conduta ou atividade que se constitua em violação das disposições da Lei Anticorrupção (Lei 12.846/13), eventuais alterações e regulamentações pertinentes.

11.2. As Partes, por si e por seus administradores, diretores, funcionários e agentes, bem como seus sócios, que venham a agir em seu nome, se obrigam a conduzir suas práticas comerciais de forma ética e em conformidade com os preceitos legais aplicáveis.

11.3. Na execução do objeto deste contrato é vedado dar, oferecer, pagar, prometer pagar, ou autorizar o pagamento direta ou indiretamente, de dinheiro ou qualquer

coisa de valor à autoridade governamental, consultores, representantes, parceiros, ou quaisquer terceiros, com a finalidade de influenciar qualquer ato ou decisão do agente ou do governo, ou para assegurar qualquer vantagem indevida, ou direcionar negócios para qualquer pessoa, em violação aos dispositivos da Lei Anticorrupção.

CLÁUSULA 12ª – DAS DISPOSIÇÕES GERAIS

12.1. A tolerância das Partes não implica novação das obrigações assumidas no presente contrato.

12.2. Fica eleito o foro da Comarca de Indaiatuba como competente para apreciar todas as questões decorrentes do presente contrato, com renúncia expressa de qualquer outro, por mais privilegiado que for.

12.3. As Partes declaram para todos os efeitos serem independentes, de forma que a presente contratação não tem caráter exclusivo e não criará vínculo, de natureza empregatícia, previdenciária ou como agente comercial, sociedade subsidiária, coligada ou representação legal.

12.4. As Partes concordam e aceitam que o presente instrumento poderá ser firmado através de assinatura eletrônica, devidamente regulamentada pela Medida Provisória 2.200-2/2001, com a qual as partes declaram ciência e concordância.

12.5. Os signatários abaixo identificados declaram ser legal e formalmente habilitados para assinar este instrumento em nome das Partes, sob pena de responderem solidariamente em nome próprio por qualquer débito ou infração deste proveniente.

12.6. Em caso de contradição entre os termos deste contrato e dos seus anexos, prevalecerá, nesta ordem, o disposto neste instrumento, na Proposta da CONTRATADA e no Termo de Referência.

E por estarem assim justas e de pleno acordo no que se refere aos termos do presente contrato, firmam o mesmo e assinam o Termo de Ciência e de Notificação do Tribunal de Contas do Estado, ao final do presente contrato.

Indaiatuba, aos __ de _____ de ____.

Antonio Corrêa
SUPERINTENDENTE - SEPREV
CONTRATANTE

_____
CONTRATADA

Gestor(a):

_____

Fiscal Técnico e Administrativo:

_____

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: **SEPREV – SERVIÇO DE PREVIDÊNCIA E ASSISTÊNCIA À SAÚDE DOS SERVIDORES MUNICIPAIS DE INDAIATUBA**
CONTRATADA:
CONTRATO Nº (DE ORIGEM): __/**2024**
OBJETO: **CONTRATAÇÃO DE SOLUÇÃO INTEGRADA DE FIREWALL NEXT GENERATION, COM SISTEMA REDUNDANTE EM ALTA DISPONIBILIDADE, CONTEMPLANDO O FORNECIMENTO DE EQUIPAMENTOS E DE LICENÇAS, PARA PREVENÇÃO DE ATAQUES CIBERNÉTICOS E PROTEÇÃO DOS DADOS E INFORMAÇÕES DOS COMPUTADORES E SERVIDORES DE ARQUIVOS DO SEPREV, POR UM PERÍODO DE 12 (DOZE) MESES.**
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 nº 01/2020, 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:

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.

Indaiatuba, aos __ de _____ de 2024.

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:

Nome: Antonio Corrêa
Cargo: Superintendente
CPF: 107.837.418-04

RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME OU RATIFICAÇÃO DA DISPENSA/INEXIGIBILIDADE DE LICITAÇÃO:

Nome: Antonio Corrêa

Cargo: Superintendente
CPF: 107.837.418-04
Assinatura:

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:
Pelo contratante:

Nome: Antonio Corrêa
Cargo: Superintendente
CPF: 107.837.418-04
Assinatura:

Pela contratada:
Nome:
Cargo:
CPF:
Assinatura:

ORDENADOR DE DESPESAS DA CONTRATANTE:
Nome: Antonio Corrêa
Cargo: Superintendente
CPF: 107.837.418-04
Assinatura:

GESTOR(ES) DO CONTRATO:
Nome:
Cargo:
CPF:
Assinatura:

FISCAL TÉCNICO E ADMINISTRATIVO:
Nome:
Cargo:
CPF:
Assinatura:

DECLARAÇÃO DE DOCUMENTOS À DISPOSIÇÃO DO TCE-SP

CONTRATANTE: **SEPREV – SERVIÇO DE PREVIDÊNCIA E ASSISTÊNCIA À SAÚDE DOS SERVIDORES MUNICIPAIS DE INDAIATUBA**

CNPJ Nº: **68.004.118/0001-21**

CONTRATADA:

CNPJ Nº:

CONTRATO N° (DE ORIGEM): __/**2024**

DATA DA ASSINATURA: __/__/**2024**

VIGÊNCIA: __/__/**2024 a** __/__/**2025**

OBJETO: **CONTRATAÇÃO DE SOLUÇÃO INTEGRADA DE FIREWALL NEXT GENERATION, COM SISTEMA REDUNDANTE EM ALTA DISPONIBILIDADE, CONTEMPLANDO O FORNECIMENTO DE EQUIPAMENTOS E DE LICENÇAS, PARA PREVENÇÃO DE ATAQUES CIBERNÉTICOS E PROTEÇÃO DOS DADOS E INFORMAÇÕES DOS COMPUTADORES E SERVIDORES DE ARQUIVOS DO SEPREV, POR UM PERÍODO DE 12 (DOZE) MESES.**

VALOR:

Declaro(amos), na qualidade de responsável(is) pela entidade supra epigrafada, sob as penas da Lei, que os demais documentos originais, atinentes à correspondente licitação, encontram-se no respectivo processo administrativo arquivado na origem à disposição do Tribunal de Contas do Estado de São Paulo, e serão remetidos quando requisitados.

Indaiatuba, aos __ de _____ de 2024.

Antonio Corrêa
Superintendente

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: F82A-E0E2-E268-8900

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

THAIANE APARECIDA DOS SANTOS ALMEIDA (CPF 446.XXX.XXX-74) em 04/09/2024 12:30:37 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

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

https://seprev.1doc.com.br/verificacao/F82A-E0E2-E268-8900