

**PREGÃO ELETRÔNICO Nº 90.010/2026**  
**AMPLA CONCORRÊNCIA**

PROCESSO : TC/001321/2026  
MODALIDADE : PREGÃO ELETRÔNICO  
CONTRATANTE : TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO  
UASG : 925462  
OBJETO : Contratação de solução tecnológica de segurança da informação, composta por *hardware*, *software* e serviços especializados, para fortalecimento da infraestrutura de cibersegurança do TCMSP, incluindo fornecimento de equipamentos *FortiGate 201G* ou superior e componentes integrados, serviços de suporte, instalação, configuração, manutenção e banco de horas técnicas.  
TIPO : **MENOR PREÇO GLOBAL**  
LOCAL DA SESSÃO : Portal de Compras do Governo Federal –  
PÚBLICA <https://www.gov.br/compras/pt-br/>  
DATA DE ABERTURA : **17 de junho de 2026**  
HORÁRIO : **9h00**

O **TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO**, com sede na Avenida Professor Ascendino Reis nº 1130, Vila Clementino, nesta Capital, torna público, para conhecimento de quantos possam interessar, que, em obediência ao que preceituam a Lei Federal nº 14.133, de 1º de abril de 2021, Leis Complementares nº 123/06, 147/14 e 155/16, os Decretos Municipais nº 62.100 de 27 de dezembro de 2022 e nº 56.475, de 05 de outubro de 2015, a Instrução Normativa nº 2, de 27 de janeiro de 2023, da Secretaria Municipal de Gestão, e demais normas pertinentes, fará realizar licitação na modalidade **PREGÃO**, na forma **ELETRÔNICA**, a ser processada pelo Pregoeiro do Tribunal, o qual terá como critério de julgamento o **MENOR PREÇO GLOBAL**, em conformidade com as disposições deste Edital e respectivos anexos.

## **1. DO OBJETO**

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de solução tecnológica de segurança da informação, composta por *hardware*, *software* e serviços especializados, para fortalecimento da infraestrutura de cibersegurança do TCMSP, incluindo fornecimento de equipamentos *FortiGate 201G* ou superior e componentes integrados, serviços de suporte, instalação, configuração, manutenção e banco de horas técnicas, conforme especificações e quantidades constantes neste edital e seus anexos.

## **2. DOS RECURSOS ORÇAMENTÁRIOS**

2.1. As despesas resultantes do presente instrumento correrão por conta dos recursos constantes das dotações **10.10.01.126.4001.2171.3390.40 – Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica**, **77.10.01.126.4002.2818.4490.52 – Equipamentos e Material Permanente e 77.10.01.126.4002.2818.3390.40 – Serviços de Tecnologia da Informação e comunicação – Pessoa Jurídica**.

## **3. DO CREDENCIAMENTO**

3.1. O Credenciamento é o nível básico do registro cadastral no Sistema de Cadastramento Unificado de Fornecedores – SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica, e dar-se-á pela atribuição, pelo órgão provedor, de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico.

3.2. O cadastro no SICAF poderá ser iniciado no Portal de Compras do Governo Federal, no sítio <https://www.gov.br/compras/pt-br/>, com a solicitação de *login* e senha pelo interessado.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante, ou de seu representante legal, e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema, ou ao Tribunal de Contas do Município de São Paulo, promotor da licitação, responsabilidade por eventuais danos decorrentes de uso indevido de suas credenciais de acesso, ainda que por terceiros.

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

3.6. Nenhuma pessoa, ainda que munida de procuração, poderá representar mais de uma empresa no presente certame, sob pena de exclusão sumária das representadas.

## **4. DA PARTICIPAÇÃO NO PREGÃO**

4.1. Poderão participar deste Pregão interessados com ramo de atividade compatível com o objeto desta licitação.

4.2. Será admitida a participação de pessoas jurídicas reunidas em consórcios, nos termos do artigo 15 da Lei n. 14.133/21.

4.2.1. O consórcio deverá entregar, juntamente com os documentos de habilitação:

4.2.1.1. Compromisso público ou particular de constituição de consórcio, subscrito pelos consorciados;

4.2.1.2. Documento com indicação da empresa líder pelo consórcio, que será responsável por sua representação perante o TCMSP.

4.2.1.3. Será admitido, para efeito de qualificação técnica, quando exigido, o somatório dos quantitativos de cada consorciado.

4.2.2. A empresa consorciada é impedida de participar, no presente certame, em mais de um consórcio ou de forma isolada;

4.2.3. Os integrantes do consórcio respondem, de forma solidária, pelos atos praticados em consórcio, tanto na fase de licitação, quanto na de execução do contrato.

4.2.4. A empresa líder será a representante do consórcio perante a CONTRATANTE e deverá subscrever a proposta de preços, em nome do consórcio.

4.2.5. O prazo de duração do consórcio deve, no mínimo, coincidir com o prazo de vigência do contrato.

4.2.6. Tratando-se de consórcio, o licitante vencedor fica obrigado a promover, antes da celebração do contrato, a constituição e o registro do consórcio no órgão oficial competente, nos termos do compromisso.

4.2.7. A substituição de consorciado deverá ser expressamente autorizada pelo TCMSP e condicionada à comprovação de que a nova empresa do consórcio possua, no mínimo, os mesmos quantitativos, para efeito de qualificação técnica, se exigida, apresentados pela empresa substituída, para fins de habilitação do consórcio no processo licitatório que originou o contrato.

4.3. Não poderão participar desta licitação:

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

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

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

4.3.3. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do TCMSP, ou com agente público que desempenhe função no processo de licitação ou que 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;

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

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

4.3.6. agente público do TCMSP;

4.3.6.1. Essa vedação estende-se a terceiro que auxilie na condução da contratação, na

qualidade de integrante de equipe de apoio, profissional especializado ou funcionário, ou representante de empresa que preste assessoria técnica.

4.4. Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes **declarações**:

4.4.1. Que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123/2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

4.4.1.1. A assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa ou empresa de pequeno porte;

4.4.1.2. A falsidade das declarações prestadas, objetivando os benefícios da Lei Complementar nº 123/2006, poderá caracterizar o crime de que trata o art. 299 do Código Penal, sem prejuízo do enquadramento em outras figuras penais e das sanções administrativas previstas na legislação pertinente, mediante o devido processo legal, e implicará, também, o afastamento do licitante, se o fato vier a ser constatado durante o trâmite da licitação.

4.4.2. Que está ciente e concorda com as condições contidas no Edital e seus anexos, respondendo pela veracidade das informações prestadas, na forma da lei.

4.4.3. Que a proposta econômica compreenderá a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal de 1988, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data da sua entrega em definitivo.

## **5. DO ENVIO DA PROPOSTA ELETRÔNICA**

5.1. O licitante deverá registrar o(s) valor(es) da(s) sua(s) proposta(s), no sistema eletrônico, até a data e horário marcados para abertura da sessão, quando, então, encerrar-se-á automaticamente a etapa de envio dessa proposta.

5.2. O envio da proposta ocorrerá por meio de chave de acesso e senha.

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

5.4. O licitante será responsável por todas as transações que forem efetuadas em seu nome, no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

5.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico, durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema, de sua desconexão ou por sua omissão quando chamado à manifestação via “chat”.

5.6. Até a abertura da sessão, os licitantes poderão retirar ou substituir as propostas apresentadas.

5.7. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, do campo “**valor unitário**” correspondente ao **valor de todos os itens, para toda a vigência contratual**, considerando a prestação integral do objeto, de acordo com os preços praticados no mercado, conforme

estabelece o art. 23 da Lei 14.133/21, em algarismo, expresso em moeda corrente nacional (R\$), considerando as características constantes do Anexo I deste Edital.

5.8. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente sobre o objeto a ser contratado, por este Edital.

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

## **6. DA ABERTURA DA SESSÃO E FORMULAÇÃO DE LANCES**

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

6.2. Iniciada a etapa competitiva, os licitantes poderão oferecer lances sucessivos, exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivos horário de registro e valor.

6.3. O lance deverá ser ofertado pelo **valor global do objeto**, nos termos estabelecidos no item 5.7.

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

6.4.1. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta, será de **R\$0,01 (um centavo)**;

6.5. Será adotado para o envio de lances, no pregão eletrônico, o modo de disputa **“aberto e fechado”**, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

6.6. A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até 10 (dez) minutos, aleatoriamente determinado.

6.7. Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que, em até 05 (cinco) minutos, o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final, sigiloso até o encerramento deste prazo.

6.7.1. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até 05 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

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

6.8.1. Não havendo lance final e fechado classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada, para que os demais licitantes, até o máximo de 03 (três), na ordem de classificação, possam ofertar, em até 05 (cinco) minutos, um lance final e fechado, o qual será sigiloso até o encerramento deste prazo.

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

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

6.10.1. Quando a desconexão do sistema eletrônico, para o Pregoeiro, persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente depois de decorridas 24 (vinte e quatro) horas após a comunicação do fato aos participantes, no portal de Compras do Governo Federal – “Compras.gov.br”.

6.11. O critério de julgamento adotado será o **menor preço global**, conforme definido neste Edital e seus anexos.

6.12. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta e, na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.

6.13. Encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará, em coluna própria, as microempresas e empresas de pequeno porte, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto Municipal nº 56.475, de 05 de outubro de 2015.

6.13.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço serão consideradas empatadas com a primeira colocada.

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

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

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

6.14. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

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

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

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

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

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

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

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

6.14.2.2. empresas brasileiras;

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

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

6.15. Encerrada a etapa de envio de lances da sessão pública, o Pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

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

6.16. Sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida.

6.17. Concluída a fase de negociação, o Pregoeiro procederá à análise da proposta classificada em primeiro lugar, verificando a compatibilidade do preço apresentado com o valor máximo estabelecido para a contratação, conforme previsto neste Edital e seus anexos.

## **7. DO ENCAMINHAMENTO E JULGAMENTO DA PROPOSTA**

7.1. O licitante detentor da melhor oferta, no prazo de 02 (duas) horas, contado da solicitação efetuada no sistema eletrônico, sob pena de desclassificação, deverá encaminhar sua **proposta final**, conforme modelo do Anexo II, a qual deverá:

7.1.1. Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada pelo licitante ou seu representante legal;

7.1.2. Indicar nome ou razão social da proponente, nº do CNPJ, endereço completo, telefone, e-mail, bem como o nome e nº do CPF e/ou RG de seu representante legal;



- 7.1.3. Conter a especificação detalhada do objeto ofertado;
- 7.1.4. Ter validade não inferior a 60 (sessenta) dias, contados a partir da data de sua apresentação;
- 7.1.5. Conter a indicação do banco, número da conta e agência do licitante detentor da melhor proposta, para fins de pagamento;
- 7.1.6. **Constar preço unitário e total, por item, e global, para o período da vigência contratual,** expressos em Real (R\$), em algarismos, com apenas duas casas após a vírgula, computados todos os custos, inclusive frete e demais encargos que incidam sobre o objeto.
- 7.1.7. Conter **DECLARAÇÃO** de que os produtos fornecidos serão novos, de primeiro uso, em linha de fabricação, e que os serviços técnicos especializados serão executados por profissionais habilitados e capacitados, detentores de certificados técnicos emitidos pelo fabricante.
- 7.1.8. Conter **DECLARAÇÃO** de que os serviços técnicos especializados necessários à execução do objeto contratual serão prestados por técnicos devidamente habilitados, com capacitação compatível com a complexidade da solução ofertada e com as exigências previstas no Edital e no Termo de Referência.
- 7.2. O prazo estabelecido pelo Pregoeiro poderá ser prorrogado por solicitação escrita e justificada do licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.
- 7.3. O licitante deverá, comprovadamente, possuir poderes, na forma da lei, para formular ofertas e lances de preços, bem como praticar todos os demais atos pertinentes ao certame.
- 7.4. A proposta final deverá ser documentada nos autos, devendo ser observada no decorrer da execução do contrato e na aplicação de eventual sanção à Contratada, se for o caso.
  - 7.3.1 Todas as especificações do objeto, contidas na proposta, vinculam a Contratada.
- 7.5. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.
- 7.6. Será desclassificada a proposta ou o lance vencedor que:
  - 7.6.1. Contenha vício insanável ou ilegalidade;
  - 7.6.2. Não obedeça às especificações técnicas contidas em edital;
  - 7.6.3. Não tiver sua exequibilidade demonstrada, quando exigido pela Administração;
  - 7.6.4. Apresentar desconformidade com quaisquer outras exigências do edital, desde que insanável;
  - 7.6.5. Apresentar preço final superior ao orçamento estimado ou que apresentar preço manifestamente inexequível.
    - 7.6.5.1. Considera-se **inexequível** a proposta de preços ou menor lance que, comprovadamente, 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, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele



renuncie a parcela ou à totalidade da remuneração.

7.7. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

7.8. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

## **8. DA HABILITAÇÃO**

8.1. Para participação no Pregão, referentes às informações atinentes à sua habilitação, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, informando que:

8.1.1. Atende aos requisitos de habilitação previstos em lei e no instrumento convocatório;

8.1.2. Inexiste impedimento à sua habilitação e que comunicará a superveniência de ocorrência impeditiva ao órgão ou entidade contratante;

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

8.1.4. Manifesta ciência em relação a todas as informações e condições locais para o cumprimento das obrigações objeto da licitação.

8.1.5. Cumpre o disposto no inciso XXXIII do art. 7º da Constituição Federal de 1988, que proíbe o trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesesseis anos, salvo na condição de aprendiz, a partir de quatorze anos.

8.1.6. Em cumprimento à legislação trabalhista:

8.1.6.1. Observa os incisos III e IV do art. 1º e cumpre o disposto no inciso III do art. 5º, todos da Constituição Federal de 1988, que veda o tratamento desumano ou degradante.

8.1.6.2. Cumpre a reserva de cargos prevista em lei para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, quando cabíveis.

8.2. Como condição prévia à análise da documentação de habilitação do detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará, por meio do sistema eletrônico, o eventual descumprimento das suas condições de participação, especialmente quanto à existência de sanções que impeçam sua atuação no certame ou a futura contratação, mediante consulta aos seguintes cadastros:

8.2.1. SICAF;

8.2.2. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União;

8.2.3. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça;

8.2.4. Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU;

8.2.5. Relação de empresas apenadas pelo Governo do Estado de São Paulo;

8.2.6. Relação de empresas apenadas pela Prefeitura de São Paulo.

8.3. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, inclusive de todas as empresas reunidas em consórcio, por força do art. 12 da Lei nº 8.429/1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

8.4. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

8.5. Caso atendidas as condições de participação, a habilitação dos licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômico-financeira e habilitação técnica, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

8.5.1. O interessado, para efeitos da habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018, mediante a utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas.

8.6. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

8.7. Os documentos exigidos para habilitação que não estejam contemplados no Sicafe serão enviados por meio do sistema, em formato digital, **NO PRAZO DE 02 (DUAS) HORAS**, prorrogável por igual período em caso de solicitação tempestiva e justificada, contado da solicitação do Pregoeiro.

8.8. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de máximo de 02 (duas) horas, sob pena de inabilitação.

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

8.9. Findo o prazo concedido, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

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

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

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

8.11. Não serão aceitos documentos com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

8.12. Todos os documentos deverão estar em nome do licitante e, preferencialmente, com o número do CNPJ e endereço respectivo.

8.12.1. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz;

8.12.2. Se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles que, pela própria natureza, forem comprovadamente emitidos apenas em nome da matriz;

8.12.3. Se o licitante for a matriz e a fornecedora for a filial, os documentos deverão ser apresentados em nome da matriz e da filial, simultaneamente.

8.12.4. Em caso de **consórcio**, cada um dos membros deverá comprovar, individualmente, os requisitos de habilitação e apresentar as declarações exigidas neste Edital.

8.12.4.1. Cada membro deverá, também, comprovar as exigências de qualificação econômico-financeira, salvo a comprovação de patrimônio líquido mínimo, que poderá ser atendida pelo somatório dos valores de cada consorciado.

8.13. Os licitantes poderão suprir a ausência da documentação de habilitação, que deveria constar no SICAF ou não contemplados por ele, encaminhando, nos termos deste Edital, a documentação relacionada nos itens a seguir, quando convocados, para fins de habilitação:

**8.13.1. Habilitação Jurídica:**

8.13.1.1. Comprovação de existência da pessoa jurídica e, quando cabível, da autorização para o exercício da atividade a ser contratada.

**8.13.2. Regularidade Fiscal e Trabalhista:**

8.13.2.1. Prova da inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

8.13.2.2. Prova da inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.13.2.3. Prova da regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.13.2.4. Prova da regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.13.2.5. Prova da inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943 (Certidão Negativa de Débitos Trabalhistas);

8.13.2.6. Certidão Negativa de débitos referentes a tributos estaduais relacionados com o objeto licitado, do domicílio ou sede do licitante.

8.13.2.6.1. Os licitantes com domicílio ou sede no Estado de São Paulo deverão comprovar a regularidade fiscal por meio da Certidão Negativa de Débitos Tributários da Dívida Ativa do Estado de São Paulo, expedida pela Procuradoria Geral do Estado, conforme Portaria CAT nº 20, de 1º de abril de 1998.

8.13.2.7. Prova da regularidade para com a Fazenda Municipal do domicílio ou sede do licitante, relativamente aos tributos mobiliários;

8.13.2.7.1. Caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

8.13.2.8. Os documentos referentes à regularidade fiscal e trabalhista poderão ser substituídos ou supridos, no todo ou em parte, por outros meios hábeis a comprovar a regularidade do licitante, inclusive por meio eletrônico.

8.13.2.8.1. O licitante detentor da melhor proposta, enquadrado como microempresa ou empresa de pequeno porte, deverá apresentar toda a documentação exigida para efeito de comprovação da regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

8.13.2.9. Serão aceitas como prova de regularidade certidões positivas com efeito de negativas, que noticiem em seu corpo que os débitos estão judicialmente garantidos ou com sua exigibilidade suspensa.

#### 8.13.3. Qualificação Econômico-Financeira:

8.13.3.1. **Certidão negativa de falência**, expedida pelo distribuidor do principal estabelecimento da pessoa jurídica, em data não superior a 60 (sessenta) dias da data da abertura do certame, se outro prazo não constar do documento.

8.13.3.1.1. No caso de certidão positiva, o licitante deverá juntar a Certidão de Objeto e Pé do processo, expedida pelo órgão competente, esclarecendo o posicionamento da(s) ação(ões).

8.13.3.1.2. No caso de sociedade simples, a proponente deverá apresentar certidão dos processos cíveis em andamento relativos à solvência ou não do licitante, expedido pelo distribuidor da sede de pessoa jurídica, em data não superior a 60 (sessenta) dias da data da abertura do certame, se outro prazo não constar do documento.

8.13.3.2. No caso de empresa em **Recuperação Judicial**, o licitante deverá apresentar uma **declaração/certidão**, emitida pela instância judicial competente, que comprove a homologação/deferimento do seu plano de recuperação judicial/extrajudicial pelo juízo competente, a sua vigência, e, por conseguinte, a sua boa saúde financeira.

8.14. As empresas, cadastradas ou não no SICAF, deverão apresentar ainda:

8.14.1. **DECLARAÇÃO** subscrita por quem detenha poderes de representação, se for o caso, sob as penas do art. 299 do Código Penal, de que se enquadra como microempresa, empresa de pequeno porte ou cooperativa, nos termos da Lei Complementar nº 123/2006 e do Decreto nº 56.475/2015, não se incluindo nas hipóteses de exclusão previstas no § 4º do artigo 3º da referida Lei Complementar, e que inexistem fatos supervenientes que conduzam ao seu desenquadramento dessa situação, conforme modelo constante do Anexo IV.

8.14.1.1. No caso de microempreendedor individual, a declaração poderá ser substituída pelo

Certificado de Condição de Microempreendedor Individual – CCMEI, emitido pelo Portal do Empreendedor.

8.14.2. **DECLARAÇÃO** de que está apto ou autorizado pela fabricante da solução a comercializar e a prestar suporte técnico da solução objeto do certame.

8.14.2.1. A efetiva comprovação será exigida como condição para assinatura do contrato.

8.14.2.2. A declaração poderá ser substituída por carta ou certificado emitido pelo fabricante, contrato de distribuição ou por meio de domínio público (“site”) do fabricante da oferta.

8.15. Não serão aceitos documentos com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

8.16. A comprovação da regularidade fiscal e trabalhista, da qualificação econômico-financeira e da habilitação jurídica, conforme o caso, poderá ser substituída pela consulta ao SICAF, nos casos em que a empresa estiver habilitada no referido sistema, conforme o disposto nos arts. 4º, caput, 8º, § 3º, 13 a 18 e 43, III, da Instrução Normativa SLTI/MPDG nº 2, de 11 de outubro de 2010.

8.16.1. Também poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando o licitante esteja com alguma documentação vencida junto ao SICAF.

8.16.2. Caso o Pregoeiro não logre êxito em obter a certidão correspondente através do sítio oficial, ou na hipótese de se encontrar vencida no referido sistema, o licitante será convocado a encaminhar, no prazo de 02 (duas) horas, documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação.

8.17. A existência de restrição relativamente à regularidade fiscal e trabalhista, conforme estatui o art. 43, § 1º da Lei Complementar nº 123/2006, não impede que o licitante qualificado como microempresa ou empresa de pequeno porte seja declarado vencedor, uma vez que atenda a todas as demais exigências do edital.

8.17.1. Os licitantes, ainda que pretendam apresentar sua regularidade fiscal ou trabalhista com alguma restrição, nos termos da Lei Complementar nº 123/2006, deverão declarar o cumprimento dos requisitos de habilitação, uma vez que neste Edital constam as exigências próprias para quem pretender se utilizar deste benefício, ficando, portanto, implícita a ressalva da possibilidade de apresentação de documentação afeta à regularidade fiscal com restrição e regularização “a posteriori”.

8.18. Uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal ou trabalhista, o licitante será convocado para, no prazo de 5 (cinco) dias úteis após a declaração do vencedor, nos termos da Lei Complementar nº 123/2006, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

8.18.1. A não-regularização fiscal no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, com a reabertura da sessão pública.

8.19. Na análise dos documentos de habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

8.20. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

8.21. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

8.22. No caso de inabilitação, seguir-se-á a disciplina antes estabelecida para aceitação da proposta subsequente.

8.22.1. Os documentos apresentados deverão estar com seu prazo de validade em vigor. Se este prazo não constar de cláusula específica do Edital, do próprio documento ou de lei aplicável à espécie, será considerado o prazo de validade de 06 (seis) meses, a contar da sua expedição.

8.23. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

8.24. Da sessão pública do Pregão, divulgar-se-á Ata no sistema eletrônico.

## **9. DOS RECURSOS**

9.1 O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de, no mínimo, dez minutos, para que qualquer licitante manifeste a intenção de recorrer.

9.2 Havendo manifestação, o recorrente terá o prazo de 03 (três) dias úteis para apresentar as razões, pelo sistema eletrônico, sob pena de preclusão, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões, também pelo sistema eletrônico, em outros 03 (três) dias úteis, que começarão a contar da data de intimação pessoal ou da divulgação da interposição de recurso, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

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

## **10. DA REABERTURA DA SESSÃO PÚBLICA**

10.1. A sessão pública poderá ser reaberta:

10.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam;

10.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal, nos termos do art. 43, §1º da Lei Complementar nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

10.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

10.2.1. A convocação se dará por meio do sistema eletrônico (“chat”) ou e-mail, de acordo com a fase do procedimento licitatório.

10.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo

responsabilidade do licitante manter seus dados cadastrais atualizados.

## 11. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

11.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, pela autoridade competente, que, posteriormente, homologará a licitação.

## 12. DA ASSINATURA DO CONTRATO

12.1. As obrigações decorrentes desta licitação consubstanciar-se-ão nos termos da minuta de Contrato - Anexo V.

12.2. A adjudicatária será convocada pelo Tribunal para, no prazo de 05 (cinco) dias úteis, a contar da data de convocação, assinar o Termo de Contrato.

12.3. Antes de celebrar o Contrato, o Tribunal de Contas do Município de São Paulo efetuará consulta ao Cadastro Informativo Municipal (CADIN), conforme estabelecido no inciso I, art. 3º, da Lei nº 14.094/2005, ou na Legislação que vier a substituí-la.

12.3.1. Caso exista registro de débito no CADIN, a Proponente adjudicatária estará impossibilitada de contratar com a Administração, salvo se estiver suspenso o impedimento, conforme dispositivo legal vigente, ou se a Proponente comprovar ter ajuizado ação com garantia oferecida, na forma da lei, ou ainda, comprovar estar suspensa a exigibilidade do crédito.

12.4. Antes da assinatura do contrato, o licitante vencedor deverá apresentar, além dos documentos que estiverem vencidos:

12.4.1. **O contrato social e a procuração** de plenos poderes para a sua assinatura;

12.4.2. **Comprovação** de que está apto e/ou autorizado pela fabricante da solução a comercializar solução objeto do certame.

12.4.3. No caso de empresa em **recuperação judicial ou extrajudicial**, cópia do ato de nomeação do seu administrador judicial, ou, para o caso do administrador ser pessoa jurídica, o nome do profissional responsável pela condução do processo, acompanhada de declaração do juízo ou do administrador, de que está cumprindo o plano de recuperação judicial/extrajudicial.

12.5. O prazo para a assinatura do contrato poderá ser prorrogado uma vez, desde que solicitado por escrito, antes do término, sob alegação de motivo justo que poderá ou não ser aceito pelo TCMSP.

12.6. Na hipótese do não atendimento à convocação ou havendo recusa em fazê-lo, a Administração convocará os demais licitantes, observada a ordem de classificação, independentemente das penalidades previstas neste Edital.

12.6.1. Em caso de convocação dos licitantes classificados remanescentes, deverão ser averiguadas as condições de habilitação destes.

## 13. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

13.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência e na



Minuta de Contrato, Anexos I e V.

#### **14. DO PREÇO E DAS CONDIÇÕES DE PAGAMENTO**

14.1. Conforme previsto na Minuta de Contrato – Anexo V.

#### **15. DAS SANÇÕES ADMINISTRATIVAS**

15.1. Comete infração administrativa, nos termos do art. 155 da Lei nº 14.133/2021, o licitante/contratado que:

15.1.1. Recusar, sem justificativa, a assinar o termo de contrato, aceitar/retirar o instrumento equivalente ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade da proposta;

15.1.2. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação; Deixar de entregar os documentos exigidos no certame;

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

15.1.4. Fraudar a licitação;

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

15.1.6. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

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

15.2. 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 licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

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

a) Advertência;

b) Multa de 5% (cinco por cento) até 10% (dez por cento) sobre o valor estimado da contratação;

c) Impedimento de licitar e de contratar, bem como o descredenciamento no SICAF, pelo prazo de até 03 (três) anos, nos termos do artigo 156, inciso III, combinado com o § 4º, da Lei nº 14.133/2021;

d) Declaração de inidoneidade para licitar ou contratar, pelo prazo mínimo de 03 (três) anos e máximo de 06 (seis) anos, nos termos do artigo 156, inciso IV, combinado com o § 5º, da Lei Licitatória.

15.4. A penalidade de multa pode ser aplicada cumulativamente com as sanções de advertência, impedimento de licitar e de contratar, e declaração de inidoneidade para licitar ou contratar.

15.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 14.133/2021, e subsidiariamente na Lei nº 14.141, de 27 de março de 2006 (Lei de

Processo Administrativo do Município de São Paulo).

15.6. A autoridade competente, na aplicação das sanções, levará em consideração a natureza e gravidade da infração cometida, as peculiaridades do caso concreto, as circunstâncias agravantes ou atenuantes e os danos que dela provierem para a Administração Pública;

15.7. Caberá recurso contra a aplicação das sanções de advertência, multa e impedimento de licitar e contratar, no prazo de 15 (quinze) dias úteis contado da data da intimação do interessado, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

15.8. Caberá a apresentação de pedido de reconsideração contra a aplicação da sanção de declaração de inidoneidade para licitar ou contratar, no prazo de 15 (quinze) dias úteis contado da data da intimação do interessado, o qual será dirigido ao Presidente do TCMSP, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

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

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

15.11. Incide, no processo de aplicação de penalidade, nos casos omissos, as disposições previstas no Capítulo I do Título IV da Lei federal nº 14.133/2021.

## **16. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO**

16.1. Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital ou solicitar esclarecimentos.

16.2. As impugnações ou pedidos de esclarecimento poderão ser realizadas por forma eletrônica, encaminhadas para o e-mail [claudio.barone@tcmsp.tc.br](mailto:claudio.barone@tcmsp.tc.br) ou por petição dirigida ou protocolada na Unidade Técnica de Protocolo e Autuação do TCMSP, pelo e-mail [utpa\\_protocolo@tcmsp.tc.br](mailto:utpa_protocolo@tcmsp.tc.br), de acordo com a Portaria SG nº 06/2018, publicada no DOC de 08/12/18, pág. 109.

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

16.4. Quando o acolhimento da impugnação implicar a retificação do Edital, capaz de afetar a formulação das propostas, será designada nova data para a realização do certame.

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

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

16.6. As respostas às impugnações e os esclarecimentos prestados pelo Pregoeiro serão anexados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado.

## **17. DAS DISPOSIÇÕES GERAIS**

17.1. Fica o licitante ciente de que a apresentação de proposta implica a aceitação de todas as condições deste Edital e de seus anexos, não podendo invocar desconhecimento dos termos do instrumento convocatório ou das disposições legais aplicáveis à espécie para furtar-se ao cumprimento de suas obrigações.

17.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro, por meio de publicação no Diário Oficial da Cidade de São Paulo e pelo site [www.tcm.sp.gov.br](http://www.tcm.sp.gov.br)>Licitações TCMSP.

17.3. No julgamento das propostas e da habilitação, o Pregoeiro 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.

17.4. É facultado ao Pregoeiro ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

17.4.1. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata esse subitem, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

17.5. O Presidente do TCMSP poderá revogar a licitação por razões de interesse público decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, e anulá-la em caso de ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

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

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

17.8. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e o TCMSP não será, em nenhum caso, responsabilizado por esses custos, independentemente da condução ou do resultado do processo licitatório.

17.9. Na contagem dos prazos estabelecidos neste Edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente no TCMSP.

17.10. O desatendimento de exigências formais (não essenciais) não importará a exclusão do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

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

17.12. Os casos omissos e as dúvidas surgidas serão resolvidos pelo Pregoeiro.

17.13. O Edital está disponibilizado, na íntegra, no endereço eletrônico <http://www.tcm.sp.gov.br> – Licitações TCMSP e também poderão ser obtidos gratuitamente, por solicitação pelo e-mail [claudio.barone@tcmsp.tc.br](mailto:claudio.barone@tcmsp.tc.br) ou pessoalmente mediante o pagamento correspondente ao custo da cópia reprográfica, a ser recolhido aos cofres públicos, através de guia de recolhimento, das 8h às 16h na Av. Professor Ascendino Reis, 1.130 - Vila Clementino – São Paulo/SP.

## **18. DOS ANEXOS**

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

18.1.1. Anexo I - Termo de Referência;

18.1.2. Anexo II - Modelo de proposta (subitem 7.1.1 do Edital);

18.1.3. Anexo III - Modelo de declaração de ME/EPP/Cooperativa e inexistência de fatos supervenientes, **SE CABÍVEL** (subitem 8.14.1 do Edital);

18.1.4. Anexo IV – Modelo de declarações (subitem 8.14.2 do Edital);

18.1.5. Anexo V - Minuta de Contrato

São Paulo, 22 de maio de 2026

CLAUDIO VICENTE PALADINO BARONE

Pregoeiro

## ANEXO I

### TERMO DE REFERÊNCIA

#### 1. **DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO (art. 6º, XXIII, “a” e “i” da Lei nº 14.133/2021).**

**1.1.** Contratação de solução tecnológica de segurança da informação, composta por hardware, software e serviços especializados, para fortalecimento da infraestrutura de cibersegurança do TCMSP, incluindo fornecimento de equipamentos *FortiGate 201G* ou superior e componentes integrados, serviços de suporte, instalação, configuração, manutenção e banco de horas técnicas, conforme especificações e quantitativos previstos neste Termo de Referência.

**1.2.** Este objeto será realizado através de licitação na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO.

**1.3.** Toda a solução deverá ser fornecida, configurada e instalada por uma única empresa, a fim de garantir a compatibilidade técnica dos equipamentos ofertados, seu perfeito funcionamento e atendimento centralizado para atender ao Acordo para Nível de Serviços (SLA), definido neste Termo de Referência.

ITEM	DESCRIÇÃO	QTDE.	MÉTRICA	Período (Meses)
01	<b>FIREWALL DE PRÓXIMA GERAÇÃO:</b> FORTIGATE-201G ou SUPERIOR - 10 X GE RJ45 (INCLUDING 1 X MGMT PORT, 1 X HA PORT, 8 X SWITCH PORTS), 4 X GE SFP SLOTS, 8 X 5GE RJ45, 8 X 10GE SFP+ SLOTS, NP7LITE AND CP10 HARDWARE ACCELERATED, 480GB ONBOARD SSD STORAGE.	2	Equipamento	Entrega única
02	FORTIGATE-201G ou SUPERIOR - 3 YEAR ENTERPRISE PROTECTION (IPS, AI-BASED INLINE MALWARE PREVENTION, INLINE CASB DATABASE, DLP, APP CONTROL, ADV MALWARE PROTECTION, URL/DNS/VIDEO FILTERING, ANTI-SPAM, ATTACK SURFACE SECURITY, CONVERTER SVC, FORTICARE PREMIUM).	2	Licença	36
03	FORTIGATE-201G OU SUPERIOR - 3 YEAR NEXT CALENDAR DAY DELIVERY PRIORITY RMA SERVICE (REQUIRES FORTICARE PREMIUM OR FORTICARE ELITE).	2	Licença	36
04	DATALAKE DE SEGURANÇA: FORTIANALYZER-VM SUBSCRIPTION LICENSE WITH SUPPORT 3 YEAR SUBSCRIPTION LICENSE FOR 5 GB/DAY CENTRAL LOGGING & ANALYTICS. INCLUDE FORTICARE PREMIUM SUPPORT, IOC, SECURITY AUTOMATION SERVICE AND FORTIGUARD OUTBREAK DETECTION SERVICE.	3	Licença	36
05	GERENCIADOR DE FIREWALLS: FORTIMANAGER-VM SUBSCRIPTION LICENSE WITH SUPPORT SUBSCRIPTION LICENSE FOR 10 DEVICES/VDOMS MANAGED BY FORTIMANAGER VM S-SERIES 24X7 FORTICARE SUPPORT INCLUDED.	1	Licença	36
06	FIREWALL DE PRÓXIMA GERAÇÃO VIRTUAL PARA CLOUD: SUBSCRIPTIONS LICENSE FOR FORTIGATE-VM (2 CPU) WITH ENTERPRISE BUNDLE INCLUDED.	6	Licença	36
07	SERVIÇO DE GERENCIAMENTO DE EXPOSIÇÃO A AMEAÇAS: EXTERNAL ATTACK SURFACE MONITORING, BRAND PROTECT & ADVERSARY CENTRIC INTELLIGENCE - UP TO 500 MONITORED ASSETS. FORTICARE PREMIUM SUPPORT INCLUDED 1 YEAR SUBSCRIPTION.	1	Licença	12

08	SOLUÇÃO DE SEGURANÇA PARA DESENVOLVIMENTO DE APLICAÇÕES: LACEWORK CODE SECURITY FOR 1 CODE CONTRIBUTING DEVELOPER (MINIMUM ORDER QUANTITY 20 DEVELOPERS), INCLUDES FORTICARE PREMIUM. 1 YEAR SUBSCRIPTION.	20	Licença	12
09	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	1	Serviço	Entrega Única
10	SUPORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, NOS DIAS ÚTEIS ENTRE 8H E 18H	250	Hora	12
11	SUPORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, EM DIAS NÃO ÚTEIS	150	Hora	12

## **2. DA FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (art. 6º, XXIII, “a” e “i” da Lei nº 14.133/2021).**

A aquisição de um novo modelo de firewall, representa uma ação estratégica essencial para garantir a segurança e integridade das informações que transitam na rede de computadores do TCMSP.

Utilizamos, atualmente, os equipamentos *FortiGate 300E* como solução de segurança perimetral.

Em 2014 o Tribunal de Contas do Município de São Paulo (TCMSP) utilizava a solução *SonicWall 4600*, que atingiu seu limite de capacidade, operando com mais dispositivos conectados simultaneamente, do que o recomendado pelo fabricante. Essa limitação demandou a substituição por uma solução mais robusta.

Assim, em 2019, foi realizada a aquisição dos *firewalls FortiGate 300E*, por meio do Contrato nº 21/2019, que garantiu a segurança perimetral do TCMSP nos últimos anos.

Decorridos seis anos da implantação dessa solução, os equipamentos aproximam-se do seu ciclo final de vida útil, entrando em regime de End of Life (EoL). Com o encerramento do EoL, o fabricante deixa de fornecer atualizações de segurança, patches de vulnerabilidade, novas versões de *firmware* e suporte técnico especializado, o que expõe o ambiente do TCMSP a riscos críticos de indisponibilidade e ataques cibernéticos.

Além disso, a ausência de suporte oficial inviabiliza a correção de falhas emergentes, a compatibilidade com novas tecnologias e a integração com soluções modernas de segurança. Esse cenário compromete diretamente a resiliência cibernética e aumenta a vulnerabilidade frente a ameaças avançadas, podendo gerar impactos significativos na continuidade dos serviços essenciais do Tribunal

Com o cenário futuro de fim de ciclo de vida (End of Life), além da perda do suporte oficial de *hardware* e *software*, o TCMSP ficará impossibilitado de receber **atualizações críticas de segurança**, correções de vulnerabilidades e novos recursos. Isso significa que eventuais falhas descobertas após o encerramento do ciclo não terão solução disponibilizada pelo fabricante, expondo o nosso parque a riscos de exploração por agentes maliciosos.

Adicionalmente, a impossibilidade de atualização das funcionalidades de segurança comprometerá a capacidade de defesa frente a ameaças emergentes, deixando a infraestrutura mais vulnerável a ataques avançados. Esse cenário compromete e inviabiliza a integração da atual infraestrutura com tecnologias modernas indispensáveis à defesa digital, como sistemas de *Data Loss*

*Prevention (DLP), Cloud Access Security Broker (CASB)*, automação de resposta a incidentes e inteligência contra ameaças avançadas.

A manutenção de equipamentos descontinuados dificulta o alinhamento às boas práticas internacionais de segurança da informação e à Lei Geral de Proteção de Dados (LGPD).

A aquisição de um novo modelo de *firewall* representa, portanto, uma ação estratégica essencial para garantir a segurança e integridade das informações que transitam na rede de computadores do TCMSP. Atualmente, os equipamentos *FortiGate 300E* encontram-se em fase de encerramento de ciclo de vida útil, com prazo final de suporte técnico oficial em julho de 2026 (<https://www.parkplacetechnologies.com/eosl/fortinet/fortigate-300e>). Após esse período, não haverá garantia de atualizações de *firmware*, correções de vulnerabilidades ou suporte técnico oficial, o que caracteriza risco crítico de segurança para o ambiente do TCMSP.

Diante desse contexto, a **contratação da nova solução Fortinet** apresenta-se como a alternativa mais adequada, pois garante a continuidade dos serviços críticos do TCMSP, assegura a proteção contra ameaças cibernéticas atuais e futuras, possibilita a integração com tecnologias modernas de defesa digital e preserva a conformidade com a LGPD e padrões internacionais de segurança da informação.

Trata-se, portanto, da opção que melhor atende ao interesse público, garantindo confiabilidade, disponibilidade e evolução tecnológica para a infraestrutura de segurança do Tribunal.

### **3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO (art. 6º, XXIII, “c” da Lei nº 14.133/2021).**

O ciclo de vida do objeto contempla as seguintes fases:

- **Implantação** – fornecimento, entrega, instalação física e lógica dos equipamentos e *softwares*, realização da configuração inicial, migração de regras e integração com a infraestrutura tecnológica já existente.
- **Operação** – uso contínuo da solução de segurança pela instituição, incluindo funcionalidades de *firewall* de próxima geração, prevenção contra vazamento de dados, monitoramento centralizado, análise de eventos de segurança, proteção de ambientes em nuvem e gerenciamento de exposição a ameaças externas.
- **Manutenção e Suporte** – Execução de serviços de manutenção preventiva e corretiva, atendimento de chamados técnicos, atualização de *firmwares*, *patches* e assinaturas de segurança, garantindo a plena disponibilidade e performance da solução ao longo do contrato.
- **Evolução Tecnológica** – disponibilização de atualizações de *software*, novas funcionalidades e mecanismos de inteligência artificial integrados, de modo a assegurar a constante adequação da solução frente a ameaças emergentes, bem como a conformidade com legislações e normativos de segurança da informação, tais como a LGPD.
- **Descontinuidade / Substituição** – ao final da vida útil dos equipamentos e serviços, a solução deverá permitir a migração segura de regras, configurações e registros de auditoria para novos



ambientes tecnológicos, assegurando a continuidade operacional e mitigando riscos de descontinuidade de serviços críticos.

Com esta abordagem de ciclo de vida completo, a instituição garante não apenas a aquisição de tecnologia de ponta, mas também a sua implantação estruturada, operação eficiente, manutenção proativa, evolução contínua e planejamento adequado para a substituição futura, em alinhamento às melhores práticas de gestão de ativos de segurança da informação.

#### **4. DOS REQUISITOS DA CONTRATAÇÃO (art. 6º, XXIII, “d” da Lei nº 14.133/2021).**

##### **4.1. FIREWALL DE PRÓXIMA GERAÇÃO**

###### **4.1.1. CARACTERÍSTICAS GERAIS**

- 4.1.1.1 Deve suportar, no mínimo, 26 (vinte e seis) *Gbps* de *throughput* com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- 4.1.1.2 Deve suportar, no mínimo, 11 (onze) milhões de conexões simultâneas;
- 4.1.1.3 Deve suportar, no mínimo, 400.000 (quatrocentas mil) novas conexões por segundo;
- 4.1.1.4 Deve suportar, no mínimo, 35 (trinta e cinco) *Gbps* de *throughput VPN IPSec*;
- 4.1.1.5 Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de *VPN IPSec Site-to-Site* simultâneos;
- 4.1.1.6 Deve estar licenciado para ou suportar, sem o uso de licença, no mínimo, 15.000 (quinze mil) túneis de clientes *VPN IPSec* simultâneos;
- 4.1.1.7 Deve suportar, no mínimo, 9 (nove) *Gbps* de *throughput* de *IPS*;
- 4.1.1.8 Deve suportar, no mínimo, 7 (sete) *Gbps* de *throughput* de Inspeção *SSL*;
- 4.1.1.9 Deve suportar, no mínimo, 6 (seis) *Gbps* de *throughput* com as funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, *IPS* e *antimalware*;
- 4.1.1.10 Deve possuir, pelo menos, 4 (quatro) interfaces com suporte a conectores SFP de 1 *Gigabit Ethernet*;
- 4.1.1.11 Deve possuir, pelo menos, 10 (dez) interfaces *Gigabit Ethernet* com conectores RJ45;
- 4.1.1.12 Deve possuir, pelo menos, 8 (oito) interfaces com suporte a conectores SFP+ de 10 *Gigabit Ethernet*;
- 4.1.1.13 Deve possuir 1 (uma) *Interface Ethernet* RJ45 10/100/1000 dedicada para gerenciamento;
- 4.1.1.14 Deve possuir, pelo menos, 1 (uma) interface RJ45 ou SFP/SFP+ dedicada para alta disponibilidade (*HA*);

4.1.1.15 Deve possuir unidade do tipo SSD com no mínimo 480GB para armazenamento de informações locais;

4.1.1.16 Deve estar licenciado para gerenciar até 256 (duzentos e cinquenta e seis) pontos de acesso sem fio e 64 (sessenta e quatro) *switches* simultaneamente em um único *appliance*;

4.1.1.17 Deve possuir fonte de alimentação AC redundante e *hot swap*;

4.1.1.18 Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (contextos) por *appliance*.

#### **4.1.2. FUNCIONALIDADES FIREWALL**

4.1.2.1 A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em *appliance* com funcionalidades de *Next Generation Firewall (NGFW)*, console de gerência e monitoração.

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

4.1.2.3 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-of-sale*;

4.1.2.4 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;

4.1.2.5 As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos *appliances* desde que atendam a todos os requisitos desta especificação;

4.1.2.6 Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: *Firewall*, *Traffic Shapping* e *QoS*, Filtro de Conteúdo *Web*, retenção inline de *malwares* desconhecidos, *Inline CASB*, Detecção e descoberta de vulnerabilidades de dispositivos *IoT*, *AntiSpam*, Detecção e Prevenção de Intrusos (*IPS*), *VPN IPSec*, Controle de Aplicações, Filtro de Dados e Avaliação de Risco e Compliance (*hardening*);

4.1.2.7 Deverá contemplar serviço de conversão e migração de regras e configurações, a ser usado uma única vez no momento da implantação, e que suporte como origem, no mínimo, os maiores fabricantes de firewall de próxima geração (*Checkpoint*, *Cisco*, *Fortinet*, *Palo Alto Networks*, *Sophos* e *SonicWall*);

4.1.2.8 A solução oferecida deverá incluir um recurso de análise de conformidade (*compliance*) da postura de segurança, configurações e maturidade do ambiente dos equipamentos de firewall;

4.1.2.9 A solução deverá permitir que o administrador aplique automaticamente correções necessárias em configurações que representem riscos ou vulnerabilidades para os *firewalls*.

#### 4.1.3. FUNCIONALIDADES DE REDE

- 4.1.3.1 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 4.1.3.2 Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- 4.1.3.3 Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 4.1.3.4 Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- 4.1.3.5 Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 4.1.3.6 Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1);
- 4.1.3.7 Deve suportar NAT de Destino;
- 4.1.3.8 Deve suportar NAT de Origem;
- 4.1.3.9 Deve suportar NAT dinâmico (Many-to-Many);
- 4.1.3.10 Deve suportar NAT de Origem e Destino simultaneamente;
- 4.1.3.11 Deve suportar tradução de porta (PAT);
- 4.1.3.12 Deve suportar NAT66, NAT64 e NAT46;
- 4.1.3.13 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 4.1.3.14 Deverá suportar sFlow ou Netflow;
- 4.1.3.15 Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 4.1.3.16 Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 4.1.3.17 Deve suportar o protocolo padrão da indústria VXLAN;
- 4.1.3.18 Deve implementar o protocolo ECMP;
- 4.1.3.19 Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 4.1.3.20 Enviar log para sistemas de monitoração externos;
- 4.1.3.21 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 4.1.3.22 Deve possuir mecanismos de proteção anti-spoofing;
- 4.1.3.23 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- 4.1.3.24 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 4.1.3.25 Suportar OSPF graceful restart;

- 4.1.3.26 Deve suportar Modo *Sniffer*, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.1.3.27 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 4.1.3.28 Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 4.1.3.29 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 4.1.3.30 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*;
- 4.1.3.31 Deverá possuir alta disponibilidade (*HA*), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 4.1.3.32 O modo de Alta-Disponibilidade (*HA*) deve possibilitar monitoração de falha de *link*;
- 4.1.3.33 A solução deve suportar integração nativa com *Let's Encrypt*, para obtenção de certificados válidos, de forma automática;
- 4.1.3.34 A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: *VMware ESXI*, *Cisco ACI* e *Kubernetes*;
- 4.1.3.35 Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos *firewalls*, bem como resposta a incidentes. 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, *APIs* executadas e ocorrência de eventos de rede e segurança pré-definidos;
- 4.1.3.36 Deve permitir integração nativa com threat feeds baseados em listas de *IPs*, nomes, *mac-address* e *hashes* de *malwares*, suportando a atualização dinâmica de objetos e respectivas regras de *firewall*;
- 4.1.3.37 Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- 4.1.3.38 Deverá suportar controle por zonas de segurança;
- 4.1.3.39 Deverá suportar controles de políticas por porta e protocolo;
- 4.1.3.40 Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 4.1.3.41 Controle de políticas por usuários, grupos de usuários, *IPs*, redes e zonas de segurança;
- 4.1.3.42 Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 4.1.3.43 Controle, inspeção e descryptografia de *SSL* por política para tráfego de saída (Outbound);

- 4.1.3.44 Deve descriptografar tráfego outbound em conexões negociadas com *TLS 1.2* e *TLS 1.3*;
- 4.1.3.45 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;
- 4.1.3.46 Suporte a objetos e regras *IPv6*;
- 4.1.3.47 Suporte a objetos e regras *multicast*;
- 4.1.3.48 Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

#### **4.1.4. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

- 4.1.4.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 4.1.4.2 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 4.1.4.3 Reconhecer pelo menos 4.000 (quatro mil) 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*;
- 4.1.4.4 Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
- 4.1.4.5 Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 4.1.4.6 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;
- 4.1.4.7 Para tráfego criptografado *SSL*, deve descriptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 4.1.4.8 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 específicas dentro de uma aplicação;
- 4.1.4.9 Identificar o uso de táticas evasivas via comunicações criptografadas;
- 4.1.4.10 Atualizar a base de assinaturas de aplicações automaticamente;
- 4.1.4.11 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;

- 4.1.4.12 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;
- 4.1.4.13 Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 4.1.4.14 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;
- 4.1.4.15 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 4.1.4.16 Deve alertar o usuário quando uma aplicação for bloqueada;
- 4.1.4.17 Deve possibilitar a diferenciação de tráfegos *Peer2Peer* (*Bittorrent, emule, etc*) possuindo granularidade de controle/políticas para os mesmos;
- 4.1.4.18 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (*AIM, Hangouts, Facebook Chat, etc*) possuindo granularidade de controle/políticas para os mesmos;
- 4.1.4.19 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;
- 4.1.4.20 Deve possibilitar a diferenciação de aplicações *Proxies* (*psiphon, freegate, etc*) possuindo granularidade de controle/políticas para os mesmos;
- 4.1.4.21 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*);
- 4.1.4.22 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
- 4.1.4.23 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 4.1.4.24 Deve permitir forçar o uso de portas específicas para determinadas aplicações;
- 4.1.4.25 Deve permitir filtrar vídeos de plataformas de *streaming* tais como, mas não limitando a *Youtube*;
- 4.1.4.26 Deve ter a capacidade de filtrar vídeos baseado em categorias como (*Business, Entertainment, Games, Music, Sports, News, People, LifeStyle, etc*);
- 4.1.4.27 Dever ter capacidade de filtrar vídeos por títulos de plataformas tais como, mas não limitando a *Youtube*;
- 4.1.4.28 Deve ser possível o filtro de vídeos com base na descrição do mesmo;
- 4.1.4.29 Deve ser possível criar regras de filtro de vídeos com base em expressões regulares ou *wildcard*;

4.1.4.30 Deve ter a capacidade de entregar via API com plataformas de *streaming* tais como, mas não limitando a Youtube;

4.1.4.31 Deve ser possível realizar o filtro de canais específicos permitindo que apenas vídeos desses canais possam ser acessados;

4.1.4.32 Deve ser possível configurar o *proxy* de acesso para atuar como *CASB (Cloud Access Security Broker)* em linha, inline do inglês, visando controlar o acesso a aplicações *SaaS*.

4.1.4.33 O *proxy* de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução.

#### **4.1.5. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS**

4.1.5.1 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*;

4.1.5.2 Deve incluir assinaturas de prevenção de intrusão (*IPS*) e bloqueio de arquivos maliciosos (*Antivírus* e *Anti-Spyware*);

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

4.1.5.4 Deve ser capaz de aplicar de forma complementar às assinaturas de antivírus, a inspeção online através de *Machine learning* em tempo real, bem como prevenir ataques através do bloqueio efetivo do *malware* desconhecido (Dia Zero) capaz de analisar completamente o arquivo no ambiente *sandbox*, sem que o mesmo seja entregue parcialmente ao cliente.

4.1.5.5 Deve ser capaz de analisar em tempo real através de mecanismos baseados em *Machine Learning* o tráfego de ameaças avançadas de C2 (comando e controle) e *spyware* para proteção de ameaças de dia zero.

4.1.5.6 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;

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

4.1.5.8 Deve permitir a configuração de um período para que novas assinaturas não entrem em modo de bloqueio, inibindo eventuais falsos-positivos;

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

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

4.1.5.11 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;



- 4.1.5.12 Deve permitir o bloqueio de vulnerabilidades;
- 4.1.5.13 Deve permitir o bloqueio de exploits conhecidos;
- 4.1.5.14 Deve incluir proteção contra-ataques de negação de serviços;
- 4.1.5.15 Ser imune e capaz de impedir ataques básicos como: *Syn flood*, *ICMP flood*, *UDP flood*, etc;
- 4.1.5.16 Detectar e bloquear a origem de portscans;
- 4.1.5.17 Bloquear ataques efetuados por worms conhecidos;
- 4.1.5.18 Possuir assinaturas específicas para a mitigação de ataques *DoS* e *DDoS*;
- 4.1.5.19 Possuir assinaturas para bloqueio de ataques de *buffer overflow*;
- 4.1.5.20 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 4.1.5.21 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;
- 4.1.5.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: *HTTP*, *FTP*, *SMB*, *SMTP* e *POP3*;
- 4.1.5.23 Identificar e bloquear comunicação com *botnets*;
- 4.1.5.24 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;
- 4.1.5.25 Os eventos devem identificar o país de onde partiu a ameaça;
- 4.1.5.26 Deve incluir proteção contra vírus em conteúdo *HTML* e *javascript*, *software* espião (*spyware*) e *worms*;
- 4.1.5.27 Possuir proteção contra downloads involuntários usando *HTTP* de arquivos executáveis e maliciosos;
- 4.1.5.28 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.
- 4.1.5.29 A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante
- 4.1.5.30 Deve suportar a captura de pacotes (*PCAP*), por assinatura de *IPS* ou regra de *firewall*;
- 4.1.5.31 Deve permitir que na captura de pacotes por assinaturas de *IPS* seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao

alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

4.1.5.32 A solução deve ser capaz de detectar surtos de ameaças globais, como *ransomwares*, e receber automaticamente atualizações do fabricante impedindo proativamente que essas ameaças infectem o ambiente.

#### **4.1.6. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS**

4.1.6.1 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);

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

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

4.1.6.4 Deve permitir que os usuários sejam identificados através de consulta em uma base do *Active Directory*, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

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

4.1.6.6 Deve possuir base ou cache de *URLs* local no appliance ou em nuvem do próprio fabricante, evitando *delay* de comunicação/validação das *URLs*;

4.1.6.7 Possuir pelo menos 70 (setenta) categorias de *URLs*;

4.1.6.8 Deve possuir a função de exclusão de *URLs* do bloqueio;

4.1.6.9 Permitir a customização de página de bloqueio;

4.1.6.10 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;

4.1.6.11 Deve possuir a função de proteção a resolução de endereços via *DNS*, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (*C&C*) de botnets conhecidas;

4.1.6.12 Deve possuir filtro de domínio *DNS* baseado em categorias para inspecionar o tráfego *DNS* com classificação de domínios continuamente atualizado.

#### **4.1.7. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS**

4.1.7.1 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;

- 4.1.7.2 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;
- 4.1.7.3 Deve possuir integração e suporte a *Microsoft Active Directory* para o sistema operacional *Windows Server 2012 R2* ou superior;
- 4.1.7.4 Deve permitir integração via *SAML* nas regras de *firewall*;
- 4.1.7.5 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;
- 4.1.7.6 Deve possuir integração com *Radius* para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 4.1.7.7 Deve possuir integração com *LDAP* para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 4.1.7.8 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*);
- 4.1.7.9 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;
- 4.1.7.10 Deve suportar o envio e recebimento de credenciais via *RADIUS*;
- 4.1.7.11 Deve implementar a criação de grupos customizados de usuários no *firewall*, baseado em atributos do *LDAP/AD*.

#### **4.1.8. FUNCIONALIDADE DE FILTRO DE DADOS**

- 4.1.8.1 Permitir identificar e, opcionalmente, prevenir a transferência de vários tipos de arquivos (*MS Office, PDF, etc*) identificados sobre aplicações (*HTTP, FTP, SMTP*);
- 4.1.8.2 Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 4.1.8.3 Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 4.1.8.4 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.
- 4.1.8.5 Deve funcionar de maneira que consiga impedir que dados sensíveis saiam da rede e também deve funcionar de modo que se previna que dados não requisitados entrem na sua rede;

4.1.8.6 Deve possuir uma base de dados de dicionários e de padrões de dados pré-definidos, tais como números de cartões de crédito, trechos de código fonte de software, etc. Essa base deve ser atualizada de forma automática pelo FABRICANTE da solução.

4.1.8.7 Deve permitir especificar a informação sensível a ser detectada como palavras, frases e expressões regulares.

4.1.8.8 Deve permitir a criação e armazenamento de impressões digitais (*fingerprint*) de documentos.

4.1.8.9 Deve permitir a aplicação de regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário autenticado;

4.1.8.10 Em tráfegos em que as regras definidas coincidirem, deve implementar no mínimo as seguintes ações: bloqueio, banimento e quarentena;

4.1.8.11 Deve armazenar, localmente ou na solução de gerenciamento centralizados de *logs*, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de *DLP*, em pelo menos os seguintes protocolos: *E-mail*, *HTTP* e mensageiros instantâneos.

#### **4.1.9. FUNCIONALIDADE DE DETECÇÃO E PROTEÇÃO DE DISPOSITIVOS IOT**

4.1.9.1 Deve ter a capacidade de identificar automaticamente o tipo de equipamento conectado (*profiling*), com suporte a dispositivos *IoT* (*Internet of Things*);

4.1.9.2 A identificação de dispositivos deve ser baseada em características do equipamento (Endereço *MAC*, Sistema Operacionais, entre outros) ou pelo usuário autenticado;

4.1.9.3 Deve permitir a identificação e mitigação de explorações de vulnerabilidades contra dispositivos *IoT*, realizando aplicações de patches;

4.1.9.4 A solução deve possuir uma base de dados de dispositivos *IoT*, atualizadas de forma regular e automática pelo fabricante da solução;

4.1.9.5 A solução deve ser capaz de identificar vulnerabilidades conhecidas em dispositivos *IoT*, fornecendo no mínimo os seguintes detalhes da vulnerabilidade encontrada: descrição, tipo, severidade, número do *CVE* e o *link* de referência do *CVE*.

#### **4.1.10. FUNCIONALIDADE DE GEOLOCALIZAÇÃO**

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

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

#### **4.1.11. FUNCIONALIDADE DE VPN**

4.1.11.1 Suportar VPN Site-to-Site;

4.1.11.2 Suportar *IPSec VPN*;

4.1.11.3 A VPN *IPSec* deve suportar 3DES;

- 4.1.11.4 A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 4.1.11.5 A VPN IPSEC deve suportar *Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*;
- 4.1.11.6 A VPN IPSEC deve suportar Algoritmo *Internet Key Exchange (IKEv1 e v2)*;
- 4.1.11.7 A VPN IPSEC deve suportar AES 128, 192 e 256 (*Advanced Encryption Standard*);
- 4.1.11.8 A VPN IPSEC deve suportar Autenticação via certificado *IKE PKI*;
- 4.1.11.9 Deve possuir interoperabilidade com os seguintes fabricantes: *Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall*;
- 4.1.11.10 Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSEC IPv6;
- 4.1.11.11 Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de *troubleshooting*;
- 4.1.11.12 Suportar leitura e verificação de CRL (*Certificate Revocation List*).

#### **4.1.12. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

- 4.1.12.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como *Youtube* e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*;
- 4.1.12.2 Suportar a criação de políticas de *QoS* e *Traffic Shaping* para os seguintes itens:
  - Endereço de origem;
  - Endereço de destino;
  - Usuário e grupo;
  - Por aplicações, incluindo, mas não limitado a *Skype, Bittorrent e YouTube*;
  - Por porta.
- 4.1.12.3 O *QoS* deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 4.1.12.4 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*, entre outros;
- 4.1.12.5 O *QoS* deve possibilitar a definição de fila de prioridade;
- 4.1.12.6 Suportar priorização em tempo real de protocolos de voz (*VOIP*) como *H.323, SIP, SCCP, MGCP* e aplicações como *Skype*;
- 4.1.12.7 Suportar marcação de pacotes *Diffserv*, inclusive por aplicação;
- 4.1.12.8 Suportar modificação de valores *DSCP* para o *Diffserv*;

- 4.1.12.9 Suportar priorização de tráfego usando informação de *ToS (Type of Service)*;
- 4.1.12.10 Disponibilizar estatísticas em tempo real para classes de *QoS* ou *Traffic Shaping*;
- 4.1.12.11 Deve suportar *QOS (Traffic-Shapping)*, em interface agregadas ou redundantes;
- 4.1.12.12 Deve possibilitar a definição de bandas distintas para *download* e *upload*.

#### **4.1.13. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS**

- 4.1.13.1 A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 4.1.13.2 A solução deve ser capaz de agregar vários *links* em uma interface virtual;
- 4.1.13.3 A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (*O365 Exchange, AWS, Dropbox* e etc);
- 4.1.13.4 A solução deve ser capaz de medir o status de qualidade do *link* baseando-se em critérios mínimos de latência, *jitter* e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
- 4.1.13.5 A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
- 4.1.13.6 A solução deve ser capaz de monitorar a qualidade e identificar falhas nos *links*, enviando sinais por meio de cada *link* para servidores ou aplicações, permitindo utilizar protocolos como *Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect* e *TWAMP (Two-way Active Measurement Protocol)*. Deve suportar, ainda, um método para mensurar a qualidade do tráfego de voz corporativo baseado em *MOS (Mean Opinion Score)*;
- 4.1.13.7 A solução deve possibilitar balanceamento de tráfego entre conexões *WAN*, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de *link (Spillover)*.
- 4.1.13.8 A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
  - Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
  - Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do *link* no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, *jitter*, perda de pacotes ou largura de banda;

- Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do *link* no qual a interface está conectada;
- Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do *link* no qual a interface está conectada;

4.1.13.9 A solução de balanceamento inteligente deve suportar marcação de pacotes *DSCP* nas definições e regras para o tráfego balanceado;

4.1.13.10 A solução de balanceamento inteligente de *links* deve suportar Roteamento dinâmico (*OSPFv2/v3, BGPv4/BGP4+*);

4.1.13.11 A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações *SaaS*, em Nuvem e Multimídia (*Vimeo, YouTube, Facebook* etc);

4.1.13.12 Deve possibilitar a agregação de túneis *IPsec*, realizando balanceamento por pacote entre os mesmos;

4.1.13.13 A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

4.1.13.14 A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um *link*, assim como, permitir definir a quantidade de falhas encontradas no *link* antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

4.1.13.15 A solução deve suportar nativamente conectores com clouds públicas, permitindo a extração de metadados dinâmicos para criação de objetos, facilitando a criação de regras de *firewall* e VPN;

4.1.13.16 Deve possibilitar a definição de largura de banda distintas nas interfaces para *download* e *upload*;

4.1.13.17 A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (*upload* e *download*) e nível de qualidade dos links (perda de pacote, *jitter* e latência);

4.1.13.18 Deve implementar balanceamento de link por hash do *IP* de origem;

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

4.1.13.20 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*;

4.1.13.21 O *appliance* físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de



Internet, e alternativamente, funcionar como circuito *Standby*, onde apenas seja acionado na eventualidade de falha no *link* principal;

4.1.13.22 Deve ser possível extrair informações de desempenho das verificações de saúde mediante *REST API*, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

## **4.2. DATALAKE DE SEGURANÇA**

4.2.1 Deve suportar o acesso via *SSH*, *WEB (HTTPS)* para gerenciamento da solução;

**4.2.2 A solução deve suportar receber, no mínimo, 5 (cinco) GB de logs diários, em conformidade com a subscrição prevista no item 04;**

4.2.3 A solução de gerenciamento centralizado poderá ser ofertada em formato de *appliance* físico ou *appliance* virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de *hardware* e *software (hypervisor)* necessário para funcionamento da solução;

4.2.4 Caso a solução seja entregue em *appliance* virtual, deverá ser compatível com *Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1;*

4.2.5 Caso a solução seja entregue em *appliance* virtual, não deve possuir limite na quantidade de múltiplas *vCPU*;

4.2.6 Caso a solução seja entregue em *appliance* virtual, não deve possuir limite para suporte a expansão de memória *RAM*;

4.2.7 Caso a solução seja ofertada em *appliance* físico, deverá ser em hardware do próprio fabricante;

4.2.8 A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

4.2.9 A solução deverá ser capaz de armazenar *logs* por no mínimo 12 (doze) meses;

4.2.10 Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

4.2.11 Possuir suporte para *SNMP* versão 2 e 3;

4.2.12 Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

4.2.13 Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

4.2.14 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;

4.2.15 Suporte a autenticação de usuários de acesso à plataforma via *LDAP, Radius* ou *TACACS+*;

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

- 4.2.17 Deve permitir gerar alertas de eventos a partir de *logs* recebidos;
- 4.2.18 A solução deve ter relatórios predefinidos;
- 4.2.19 Permitir importação e exportação de relatórios
- 4.2.20 Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
- 4.2.21 Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
- 4.2.22 Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
- 4.2.23 Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
- 4.2.24 Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
- 4.2.25 Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
- 4.2.26 Deve ter a capacidade de criar relatórios no formato *HTML*, *CSV*, *XML* e *PDF*;
- 4.2.27 Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço *IP*, usuário e senha;
- 4.2.28 Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
- 4.2.29 Deve possuir mecanismos de remoção automática para logs antigos;
- 4.2.30 Deve ter um mecanismo de "pesquisa detalhada" ou "*Drill-Down*" para navegar pelos relatórios em tempo real;
- 4.2.31 Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adaptá-lo de acordo com suas necessidades;
- 4.2.32 Permitir o envio por *e-mail* relatórios automaticamente;
- 4.2.33 Deve permitir que o relatório seja enviado por Email para o destinatário específico;
- 4.2.34 Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
- 4.2.35 Permitir a exibição graficamente e em tempo real da taxa de geração de *logs* para cada dispositivo gerenciado;
- 4.2.36 Deve permitir o uso de filtros nos relatórios;
- 4.2.37 Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
- 4.2.38 Permitir especificar o idioma dos relatórios criados;
- 4.2.39 Gerar alertas automáticos via e-mail, *SNMP* e *Syslog*, com base em eventos especiais em *logs*, gravidade do evento, entre outros;
- 4.2.40 Deve permitir o envio automático de relatórios para um servidor *SFTP* ou *FTP* externo;
- 4.2.41 Deve permitir o envio automático dos *logs* para um servidor *FTP* externo a solução;
- 4.2.42 Deve permitir exportar os *logs* no formato *CSV*;
- 4.2.43 Deve permitir que os arquivos de *log* sejam baixados da plataforma para uso externo;

- 4.2.44 Deve permitir a geração de *logs* de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
- 4.2.45 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;
- 4.2.46 Deve ser capaz de criar consultas *SQL* ou similares nos bancos de dados de *logs*, para uso em gráficos e tabelas em relatórios;
- 4.2.47 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;
- 4.2.48 Deve fornecer as informações da quantidade de *logs* armazenados e as estatísticas do tempo restante armazenado;
- 4.2.49 Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- 4.2.50 Deve permitir visualizar em tempo real os *logs* recebidos;
- 4.2.51 Deve permitir o encaminhamento de log no formato *syslog* e *CEF (Common Event Format)*;
- 4.2.52 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;
- 4.2.53 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;
- 4.2.54 Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;
- 4.2.55 Deve possuir um painel de operações que monitorea o envolvimento do usuário e o uso suspeito da *web* em sua rede;
- 4.2.56 Deve possuir um painel de operações que monitorea o tráfego da rede, aplicativos e *sites web*;
- 4.2.57 Deve possuir um painel de operações que monitoram a atividade da *VPN* em sua rede;
- 4.2.58 Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (*CPU*, Memória)
- 4.2.59 Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;
- 4.2.60 Deve possuir relatório de uso de aplicações e mídias sociais;
- 4.2.61 Deve possuir relatório de prevenção de perda de dados (*DLP*);
- 4.2.62 Deve possuir relatório de *VPN*, Prevenção de Intrusão (*IPS*), análise de ameaças cibernéticas;
- 4.2.63 Deve possuir relatório diário resumido de eventos e incidentes de segurança;

- 4.2.64 Deve possuir um relatório de tráfego *DNS* e *e-mail*;
- 4.2.65 Deve possuir relatório das 10 principais aplicações utilizadas na rede;
- 4.2.66 Deve possuir relatório dos 10 principais sites *web* utilizados na rede;
- 4.2.67 Deve possibilitar a visibilidade da utilização do balanceamento inteligente de *links*, mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos *links* (latência, *Jitter* e descarte de pacotes);
- 4.2.68 Deve suportar através da análise de tráfego de rede *IP*, *web* (*URL*) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;
- 4.2.69 Deve suportar através da análise de tráfego de rede *IP*, *web* (*URL*) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;
- 4.2.70 Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;
- 4.2.71 Deve suportar recursos de automação (*playbooks*) que, por meio de integrações com soluções de *firewall*, *endpoint*, *email*, *ITSM* e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;
- 4.2.72 Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;
- 4.2.73 Deve possuir um assistente integrado ao painel de operações, baseado em inteligência artificial generativa (Assistente de IA), que auxilie na investigação de incidentes, na resposta e na caça de ameaças;
- 4.2.74 O Assistente de IA deve permitir que administradores utilizem comandos em linguagem natural, a fim de facilitar a execução de tarefas;
- 4.2.75 O Assistente de IA deve ser capaz de interpretar eventos de segurança, gerar resumos detalhados, identificar potenciais impactos e fornece recomendações de remediação;
- 4.2.76 O Assistente de IA deve ser capaz de fornecer respostas contextualizadas com base nos dados coletados pela solução.

### **4.3. GERENCIADOR DE FIREWALLS**

- 4.3.1 Deve estar dimensionado e licenciado para gerenciar até 10 (dez) *Firewalls* de Próxima Geração (*NGFW*) considerando os modelos ofertados neste processo atendendo aos requisitos deste Item;
- 4.3.2 A solução de gerenciamento centralizado poderá ser ofertada em formato de *appliance* físico ou *appliance* virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de *hardware* e *software* (*hypervisor*) necessário para funcionamento da solução;

- 4.3.3 Caso a solução seja entregue em *appliance* virtual, deverá ser compatível com *Hypervisors*: *VMware ESXi 6.5*, *Microsoft Hyper-V 2012/2016/2019*, *KVM no Redhat 7.1*, *Nutanix AHV (AOS 5.10.5)*;
- 4.3.4 Caso a solução seja entregue em *appliance* virtual, não deve possuir limite na quantidade de múltiplas *vCPU*;
- 4.3.5 Caso a solução seja entregue em *appliance* virtual, não deve possuir limite para suporte a expansão de memória *RAM*;
- 4.3.6 Caso a solução seja ofertada em *appliance* físico, deverá ser em *hardware* do próprio fabricante;
- 4.3.7 A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;
- 4.3.8 Possibilitar a criação e administração de políticas de *Firewall*, Controle de Aplicação, Sistema de Prevenção a Intrusão (*IPS - Intrusion Prevention System*), Antivírus, Filtro de Conteúdo e *URL* e Balanceamento inteligente de *Links*;
- 4.3.9 Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do *link*, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;
- 4.3.10 Deve ter a capacidade de permitir o provisionamento de comunidades *VPN* e monitorar as conexões *VPN* de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;
- 4.3.11 Permitir criar templates de configuração dos dispositivos com informações de *DNS*, *SNMP*, Configurações de *LOG* e Administração;
- 4.3.12 Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- 4.3.13 A solução deve permitir o uso de *APIs RESTful* para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
- 4.3.14 Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
- 4.3.15 Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;
- 4.3.16 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 4.3.17 Permitir usar palavras chaves ou cores para facilitar identificação de regras;
- 4.3.18 Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;
- 4.3.19 Atribuir sequencialmente um número a cada regra de *firewall*, de *NAT* ou de *QoS*;
- 4.3.20 Permitir criação de regras que fiquem ativas em horário definido;

- 4.3.21 Permitir criação de regras com data de expiração;
- 4.3.22 Realizar o *backup* das configurações para permitir o retorno de uma configuração salva;
- 4.3.23 Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.
- 4.3.24 Gerar alertas automáticos via *Email*, *SNMP* e *Syslog*;
- 4.3.25 Deve ser permitido ao administrador transferir os *backups* para um servidor *FTP*, *SCP* ou *SFTP*.
- 4.3.26 Permitir *backup* das configurações e *rollback* de configuração para a última configuração salva;
- 4.3.27 Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;
- 4.3.28 Possuir um sistema de *backup*/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar *backups* da configuração em um determinado dia e hora;
- 4.3.29 Deve suportar a distribuição e instalação remota de novas versões de *software* dos equipamentos, de forma remota e centralizada;
- 4.3.30 Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
- 4.3.31 Deve suportar autenticação de administradores em base local e de modo remoto por meio de *RADIUS*, *LDAP*, *TACACS+* e *PKI*.
- 4.3.32 A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os *appliances* controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos *appliances* através dessa ferramenta.
- 4.3.33 A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de *software* dos *appliances*.
- 4.3.34 Deve suportar o gerenciamento de pontos de acesso de forma centralizada.
- 4.3.35 Deve suportar o gerenciamento centralizado de *switches*.
- 4.3.36 A solução deve possuir garantia, suporte e atualizações ao *software* durante a vigência do contrato.
- 4.3.37 Deve possuir um assistente integrado ao painel de operações, baseado em inteligência artificial generativa (Assistente de IA), que auxilie na configuração do ambiente, na configuração de funcionalidades de *VPN* e na investigação de problemas no ambiente gerenciado;
- 4.3.38 O Assistente de IA deve permitir que administradores utilizem comandos em linguagem natural, a fim de facilitar a execução de tarefas;
- 4.3.39 O Assistente de IA deve interpretar o estado dos dispositivos gerenciados e, em caso de ser encontrado algum problema, recomendar ações corretivas;

4.3.40 O Assistente de IA deve ter a capacidade de criar e revisar *scripts* de configurações antes de serem aplicados na solução de gerência centralizada;

#### 4.4. FIREWALL DE PRÓXIMA GERAÇÃO VIRTUAL PARA CLOUD

##### 4.4.1. CARACTERÍSTICAS GERAIS

4.4.1.1. Deve ser do tipo *appliance* virtual, sendo de responsabilidade da contratante a disponibilização dos recursos necessários para a implantação da solução: *hardware* e *software* (*hypervisor*), ou contratação de instâncias de computação em nuvem;

4.4.1.2. Deve suportar a implantação em nuvens privadas e públicas;

4.4.1.3. Em nuvens privadas, deverá ser compatível com pelo menos os *Hypervisors*: *VMware ESXi 5.5* e superiores, *Microsoft Hyper-V 2008 R2* e superiores, *Citrix XenServer 5.6 sp2* e superiores, *Linux KVM (Red Hat/CentOS 6.4* e superiores, *Ubuntu 16.04* e superiores), *Nutanix AHV 5.10* e superiores,;

4.4.1.4. Em nuvens públicas, deverá ser compatível com pelo menos as seguintes provedoras de nuvem: *AWS*, *Azure*, *Google Cloud* e *OCI*;

4.4.1.5. Deve possuir suporte, no mínimo, a 2 (duas) *vCPUs*;

4.4.1.6. O *appliance* virtual não deve possuir limite para suporte a expansão de memória *RAM*;

##### 4.4.2. FUNCIONALIDADES PARA FIREWALLS DE PRÓXIMA GERAÇÃO

4.4.2.1 A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em *appliance* com funcionalidades de *Next Generation Firewall (NGFW)*, console de gerência e monitoração.

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

4.4.2.3 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-of-sale*;

4.4.2.4 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;

4.4.2.5 As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos *appliances* desde que atendam a todos os requisitos desta especificação;

4.4.2.6 Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: *Firewall*, *Traffic Shapping* e *QoS*, Filtro de Conteúdo *Web*, retenção inline de *malwares* desconhecidos, *Inline CASB*, Detecção e descoberta de vulnerabilidades de



dispositivos *IoT*, *AntiSpam*, Detecção e Prevenção de Intrusos (*IPS*), *VPN IPSec*, Controle de Aplicações, Filtro de Dados e Avaliação de Risco e Compliance (*hardening*);

4.4.2.7 Deverá contemplar serviço de conversão e migração de regras e configurações, a ser usado uma única vez no momento da implantação, e que suporte como origem, no mínimo, os maiores fabricantes de *firewall* de próxima geração (*Checkpoint*, *Cisco*, *Fortinet*, *Palo Alto Networks*, *Sophos* e *SonicWall*);

4.4.2.8 A solução oferecida deverá incluir um recurso de análise de conformidade (*compliance*) da postura de segurança, configurações e maturidade do ambiente dos equipamentos de *firewall*;

4.4.2.9 A solução deverá permitir que o administrador aplique automaticamente correções necessárias em configurações que representem riscos ou vulnerabilidades para os *firewalls*.

#### **4.4.3 FUNCIONALIDADES DE REDE**

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

4.4.3.2 Os dispositivos de proteção de rede devem possuir suporte a *Vlans*;

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

4.4.3.4 Os dispositivos de proteção de rede devem possuir suporte a *DHCP Cliente*, *Server* e *Relay*;

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

4.4.3.6 Deve possuir a funcionalidade de tradução de endereços estáticos - *NAT (Network Address Translation)*, um para um (1-to-1), N-para-um (N-to-1);

4.4.3.7 Deve suportar *NAT* de Destino;

4.4.3.8 Deve suportar *NAT* de Origem;

4.4.3.9 Deve suportar *NAT* dinâmico (*Many-to-Many*);

4.4.3.10 Deve suportar *NAT* de Origem e Destino simultaneamente;

4.4.3.11 Deve suportar tradução de porta (*PAT*);

4.4.3.12 Deve suportar *NAT66*, *NAT64* e *NAT46*;

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

4.4.3.14 Deverá suportar *sFlow* ou *Netflow*;

4.4.3.15 Deve possuir suporte a criação de sistemas virtuais no mesmo *appliance* e que possam ser administrados por equipes distintas;

4.4.3.16 Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

- 4.4.3.17 Deve suportar o protocolo padrão da indústria *VXLAN*;
- 4.4.3.18 Deve implementar o protocolo *ECMP*;
- 4.4.3.19 Deve permitir monitorar via *SNMP* o uso de *CPU*, memória, espaço em disco, *VPN*, situação do *cluster* e violações de segurança;
- 4.4.3.20 Enviar *log* para sistemas de monitoração externos;
- 4.4.3.21 Deve haver a opção de enviar *logs* para os sistemas de monitoração externos via protocolo *SSL*;
- 4.4.3.22 Deve possuir mecanismos de proteção *anti-spoofing*;
- 4.4.3.23 Para *IPv4*, deve suportar roteamento estático e dinâmico (*RIPv2*, *BGP4* e *OSPFv2*);
- 4.4.3.24 Para *IPv6*, deve suportar roteamento estático e dinâmico (*OSPFv3*);
- 4.4.3.25 Suportar *OSPF graceful restart*;
- 4.4.3.26 Deve suportar Modo *Sniffer*, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.4.3.27 Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 4.4.3.28 Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 4.4.3.29 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 4.4.3.30 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*;
- 4.4.3.31 Deverá possuir alta disponibilidade (*HA*), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 4.4.3.32 O modo de Alta-Disponibilidade (*HA*) deve possibilitar monitoração de falha de *link*;
- 4.4.3.33 A solução deve suportar integração nativa com *Let's Encrypt*, para obtenção de certificados válidos, de forma automática;
- 4.4.3.34 A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: *VMware ESXI*, *Cisco ACI* e *Kubernetes*; Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls, bem como resposta a incidentes.
- 4.4.3.35 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, *APIs* executadas e ocorrência de eventos de rede e segurança pré-definidos;
- 4.4.3.36 Deve permitir integração nativa com threat feeds baseados em listas de *IPs*, nomes, *mac-address* e *hashes* de *malwares*, suportando a atualização dinâmica de objetos e respectivas regras de *firewall*;

- 4.4.3.37 Deverá possuir integração com *tokens* para autenticação de 02 (dois) fatores;
- 4.4.3.38 Deverá suportar controle por zonas de segurança;
- 4.4.3.39 Deverá suportar controles de políticas por porta e protocolo;
- 4.4.3.40 Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 4.4.3.41 Controle de políticas por usuários, grupos de usuários, *IPs*, redes e zonas de segurança;
- 4.4.3.42 Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 4.4.3.43 Controle, inspeção e descryptografia de SSL por política para tráfego de saída (*Outbound*);
- 4.4.3.44 Deve descryptografar tráfego *outbound* em conexões negociadas com *TLS 1.2* e *TLS 1.3*;
- 4.4.3.45 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;
- 4.4.3.46 Suporte a objetos e regras *IPv6*;
- 4.4.3.47 Suporte a objetos e regras *multicast*;
- 4.4.3.48 Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

#### **4.4.4 FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES**

- 4.4.4.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 4.4.4.2 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 4.4.4.3 Reconhecer pelo menos 4.000 (quatro mil) 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*;
- 4.4.4.4 Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
- 4.4.4.5 Deve inspecionar o *payload* de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 4.4.4.6 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*;
- 4.4.4.7 Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;

- 4.4.4.8 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 específicas dentro de uma aplicação;
- 4.4.4.9 Identificar o uso de táticas evasivas via comunicações criptografadas;
- 4.4.4.10 Atualizar a base de assinaturas de aplicações automaticamente;
- 4.4.4.11 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;
- 4.4.4.12 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;
- 4.4.4.13 Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 4.4.4.14 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;
- 4.4.4.15 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 4.4.4.16 Deve alertar o usuário quando uma aplicação for bloqueada;
- 4.4.4.17 Deve possibilitar a diferenciação de tráfegos *Peer2Peer* (*Bittorrent*, *emule*, etc) possuindo granularidade de controle/políticas para os mesmos;
- 4.4.4.18 Deve possibilitar a diferenciação de tráfegos de *Instant Messaging* (*AIM*, *Hangouts*, *Facebook Chat*, etc) possuindo granularidade de controle/políticas para os mesmos;
- 4.4.4.19 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*;
- 4.4.4.20 Deve possibilitar a diferenciação de aplicações *Proxies* (*psiphon*, *freegate*, etc) possuindo granularidade de controle/políticas para os mesmos;
- 4.4.4.21 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);
- 4.4.4.22 Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;
- 4.4.4.23 Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 4.4.4.24 Deve permitir forçar o uso de portas específicas para determinadas aplicações;

- 4.4.4.25 Deve permitir filtrar vídeos de plataformas de *streaming* tais como, mas não limitando a *Youtube*;
- 4.4.4.26 Deve ter a capacidade de filtrar vídeos baseado em categorias como (*Business, Entertainment, Games, Music, Sports, News, People, LifeStyle*, etc);
- 4.4.4.27 Dever ter capacidade de filtrar vídeos por títulos de plataformas tais como, mas não limitando a *Youtube*;
- 4.4.4.28 Deve ser possível o filtro de vídeos com base na descrição do mesmo;
- 4.4.4.29 Deve ser possível criar regras de filtro de vídeos com base em expressões regulares ou *wildcard*;
- 4.4.4.30 Deve ter a capacidade de entregar via *API* com plataformas de *streaming* tais como, mas não limitando a *Youtube*;
- 4.4.4.31 Deve ser possível realizar o filtro de canais específicos permitindo que apenas vídeos desses canais possam ser acessados;
- 4.4.4.32 Deve ser possível configurar o *proxy* de acesso para atuar como *CASB (Cloud Access Security Broker)* em linha, inline do inglês, visando controlar o acesso a aplicações *SaaS*.
- 4.4.4.33 O *proxy* de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução.

#### **4.4.5 FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS**

- 4.4.5.1 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*;
- 4.4.5.2 Deve incluir assinaturas de prevenção de intrusão (*IPS*) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware*);
- 4.4.5.3 Deve sincronizar as assinaturas de *IPS*, Antivírus, *Anti-Spyware* quando implementado em alta disponibilidade;
- 4.4.5.4 Deve ser capaz de aplicar de forma complementar às assinaturas de antivírus, a inspeção online através de *Machine learning* em tempo real, bem como prevenir ataques através do bloqueio efetivo do *malware* desconhecido (Dia Zero) capaz de analisar completamente o arquivo no ambiente *sandbox*, sem que o mesmo seja entregue parcialmente ao cliente.
- 4.4.5.5 Deve ser capaz de analisar em tempo real através de mecanismos baseados em *Machine Learning* o tráfego de ameaças avançadas de C2 (comando e controle) e *spyware* para proteção de ameaças de dia zero.
- 4.4.5.6 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;

- 4.4.5.7 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 4.4.5.8 Deve permitir a configuração de um período para que novas assinaturas não entrem em modo de bloqueio, inibindo eventuais falsos-positivos;
- 4.4.5.9 Deve ser possível a criação de políticas por usuários, grupos de usuários, *IPs*, redes ou zonas de segurança;
- 4.4.5.10 Exceções por *IP* de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
- 4.4.5.11 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;
- 4.4.5.12 Deve permitir o bloqueio de vulnerabilidades;
- 4.4.5.13 Deve permitir o bloqueio de *exploits* conhecidos;
- 4.4.5.14 Deve incluir proteção contra-ataques de negação de serviços;
- 4.4.5.15 Ser imune e capaz de impedir ataques básicos como: *Syn flood*, *ICMP flood*, *UDP flood*, etc;
- 4.4.5.16 Detectar e bloquear a origem de *portscans*;
- 4.4.5.17 Bloquear ataques efetuados por *worms* conhecidos;
- 4.4.5.18 Possuir assinaturas específicas para a mitigação de ataques *DoS* e *DDoS*;
- 4.4.5.19 Possuir assinaturas para bloqueio de ataques de buffer *overflow*;
- 4.4.5.20 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 4.4.5.21 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;
- 4.4.5.22 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: *HTTP*, *FTP*, *SMB*, *SMTP* e *POP3*;
- 4.4.5.23 Identificar e bloquear comunicação com *botnets*;
- 4.4.5.24 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;
- 4.4.5.25 Os eventos devem identificar o país de onde partiu a ameaça;
- 4.4.5.26 Deve incluir proteção contra vírus em conteúdo *HTML* e *javascript*, *software* espião (*spyware*) e *worms*;
- 4.4.5.27 Possuir proteção contra downloads involuntários usando *HTTP* de arquivos executáveis e maliciosos;

4.4.5.28 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;

4.4.5.29 A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;

4.4.5.30 Deve suportar a captura de pacotes (*PCAP*), por assinatura de *IPS* ou regra de *firewall*;

4.4.5.31 Deve permitir que na captura de pacotes por assinaturas de *IPS* seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

4.4.5.32 A solução deve ser capaz de detectar surtos de ameaças globais, como *ransomwares*, e receber automaticamente atualizações do fabricante impedindo proativamente que essas ameaças infectem o ambiente;

#### **4.4.6 FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS**

4.4.6.1 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);

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

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

4.4.6.4 Deve permitir que os usuários sejam identificados através de consulta em uma base do *Active Directory*, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

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

4.4.6.6 Deve possuir base ou cache de *URLs* local no appliance ou em nuvem do próprio fabricante, evitando *delay* de comunicação/validação das *URLs*;

4.4.6.7 Possuir pelo menos 70 (setenta) categorias de *URLs*;

4.4.6.8 Deve possuir a função de exclusão de *URLs* do bloqueio;

4.4.6.9 Permitir a customização de página de bloqueio;

4.4.6.10 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;



4.4.6.11 Deve possuir a função de proteção a resolução de endereços via *DNS*, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

4.4.6.12 Deve possuir filtro de domínio *DNS* baseado em categorias para inspecionar o tráfego *DNS* com classificação de domínios continuamente atualizado.

#### **4.4.7 FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS**

4.4.7.1 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;

4.4.7.2 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;

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

4.4.7.4 Deve permitir integração via *SAML* nas regras de *firewall*;

4.4.7.5 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;

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

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

4.4.7.8 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*);

4.4.7.9 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;

4.4.7.10 Deve suportar o envio e recebimento de credenciais via *RADIUS*;

4.4.7.11 Deve implementar a criação de grupos customizados de usuários no *firewall*, baseado em atributos do *LDAP/AD*.

#### **4.4.8 FUNCIONALIDADE DE FILTRO DE DADOS**

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

- 4.4.8.2 Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 4.4.8.3 Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 4.4.8.4 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.
- 4.4.8.5 Deve funcionar de maneira que consiga impedir que dados sensíveis saiam da rede e também deve funcionar de modo que se previna que dados não requisitados entrem na sua rede;
- 4.4.8.6 Deve possuir uma base de dados de dicionários e de padrões de dados pré-definidos, tais como números de cartões de crédito, trechos de código fonte de *software*, etc. Essa base deve ser atualizada de forma automática pelo FABRICANTE da solução.
- 4.4.8.7 Deve permitir especificar a informação sensível a ser detectada como palavras, frases e expressões regulares.
- 4.4.8.8 Deve permitir a criação e armazenamento de impressões digitais (*fingerprint*) de documentos.
- 4.4.8.9 Deve permitir a aplicação de regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário autenticado;
- 4.4.8.10 Em tráfegos em que as regras definidas coincidirem, deve implementar no mínimo as seguintes ações: bloqueio, banimento e quarentena;
- 4.4.8.11 Deve armazenar, localmente ou na solução de gerenciamento centralizados de *logs*, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de *DLP*, em pelo menos os seguintes protocolos: *E-mail*, *HTTP* e mensageiros instantâneos.

#### **4.4.9 FUNCIONALIDADE DE DETECÇÃO E PROTEÇÃO DE DISPOSITIVOS IOT**

- 4.4.9.1 Deve ter a capacidade de identificar automaticamente o tipo de equipamento conectado (*profiling*), com suporte a dispositivos *IoT* (*Internet of Things*);
- 4.4.9.2 A identificação de dispositivos deve ser baseada em características do equipamento (Endereço *MAC*, Sistema Operacionais, entre outros) ou pelo usuário autenticado;
- 4.4.9.3 Deve permitir a identificação e mitigação de explorações de vulnerabilidades contra dispositivos *IoT*, realizando aplicações de *patches*;
- 4.4.9.4 A solução deve possuir uma base de dados de dispositivos *IoT*, atualizadas de forma regular e automática pelo fabricante da solução;
- 4.4.9.5 A solução deve ser capaz de identificar vulnerabilidades conhecidas em dispositivos *IoT*, fornecendo no mínimo os seguintes detalhes da vulnerabilidade encontrada: descrição, tipo, severidade, número do *CVE* e o *link* de referência do *CVE*.

#### **4.4.10 FUNCIONALIDADE DE GEOLOCALIZAÇÃO**

- 4.4.10.1 Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 4.4.10.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

#### **4.4.11 FUNCIONALIDADE DE VPN**

- 4.4.11.1 Suportar *VPN Site-to-Site*;
- 4.4.11.2 Suportar *IPSec VPN*;
- 4.4.11.3 A *VPN IPSEC* deve suportar *3DES*;
- 4.4.11.4 A *VPN IPSEC* deve suportar Autenticação *MD5* e *SHA-1*;
- 4.4.11.5 A *VPN IPSEC* deve suportar *Diffie-Hellman Group 1, Group 2, Group 5* e *Group 14*;
- 4.4.11.6 A *VPN IPSEC* deve suportar Algoritmo *Internet Key Exchange (IKEv1 e v2)*;
- 4.4.11.7 A *VPN IPSEC* deve suportar *AES 128, 192 e 256 (Advanced Encryption Standard)*;
- 4.4.11.8 A *VPN IPSEC* deve suportar Autenticação via certificado *IKE PKI*;
- 4.4.11.9 Deve possuir interoperabilidade com os seguintes fabricantes: *Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall*;
- 4.4.11.10 Suportar *VPN* em *IPv4* e *IPv6*, assim como tráfego *IPv4* dentro de túneis *IPSec IPv6*;
- 4.4.11.11 Deve permitir habilitar e desabilitar túneis de *VPN IPSEC* a partir da interface gráfica da solução, facilitando o processo de *troubleshooting*;
- 4.4.11.12 Suportar leitura e verificação de *CRL (Certificate Revocation List)*.

#### **4.4.12 FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO**

- 4.4.12.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como *Youtube* e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*;
- 4.4.12.2 Suportar a criação de políticas de *QoS* e *Traffic Shaping* para os seguintes itens:
  - Endereço de origem;
  - Endereço de destino;
  - Usuário e grupo;
  - Por aplicações, incluindo, mas não limitado a *Skype, Bittorrent* e *YouTube*;
  - Por porta;

- 4.4.12.3 O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 4.4.12.4 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*, entre outros;
- 4.4.12.5 O QoS deve possibilitar a definição de fila de prioridade;
- 4.4.12.6 Suportar priorização em tempo real de protocolos de voz (*VOIP*) como *H.323*, *SIP*, *SCCP*, *MGCP* e aplicações como *Skype*;
- 4.4.12.7 Suportar marcação de pacotes *Diffserv*, inclusive por aplicação;
- 4.4.12.8 Suportar modificação de valores *DSCP* para o *Diffserv*;
- 4.4.12.9 Suportar priorização de tráfego usando informação de *ToS (Type of Service)*;
- 4.4.12.10 Disponibilizar estatísticas em tempo real para classes de QoS ou *Traffic Shaping*;
- 4.4.12.11 Deve suportar *QOS (Traffic-Shapping)*, em interface agregadas ou redundantes;
- 4.4.12.12 Deve possibilitar a definição de bandas distintas para *download* e *upload*.

#### **4.4.13 FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS**

- 4.4.13.1 A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 4.4.13.2 A solução deve ser capaz de agregar vários *links* em uma interface virtual;
- 4.4.13.3 A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (*O365 Exchange*, *AWS*, *Dropbox* e etc);
- 4.4.13.4 A solução deve ser capaz de medir o status de qualidade do *link* baseando-se em critérios mínimos de latência, *jitter* e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
- 4.4.13.5 A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
- 4.4.13.6 A solução deve ser capaz de monitorar a qualidade e identificar falhas nos *links*, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como *Ping*, *HTTP*, *TCP ECHO*, *UDP ECHO*, *DNS*, *TCP Connect* e *TWAMP (Two-way Active Measurement Protocol)*. Deve suportar, ainda, um método para mensurar a qualidade do tráfego de voz corporativo baseado em *MOS (Mean Opinion Score)*;
- 4.4.13.7 A solução deve possibilitar balanceamento de tráfego entre conexões *WAN*, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado

considerando os seguintes parâmetros: Sessões, Volume de tráfego, *IP* de origem e destino e Transbordo de link (*Spillover*).

4.4.13.8 A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:

4.4.13.9 Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

4.4.13.10 Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do *link* no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, *jitter*, perda de pacotes ou largura de banda;

4.4.13.11 Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do *link* no qual a interface está conectada;

4.4.13.12 Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do *link* no qual a interface está conectada;

4.4.13.13 A solução de balanceamento inteligente deve suportar marcação de pacotes *DSCP* nas definições e regras para o tráfego balanceado;

4.4.13.14 A solução de balanceamento inteligente de *links* deve suportar Roteamento dinâmico (*OSPFv2/v3*, *BGPv4/BGP4+*);

4.4.13.15 A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações *SaaS*, em Nuvem e Multimídia (*Vimeo*, *YouTube*, *Facebook* etc);

4.4.13.16 Deve possibilitar a agregação de túneis *IPsec*, realizando balanceamento por pacote entre os mesmos;

4.4.13.17 A solução deve possibilitar a criação e uso de túneis *VPN* de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

4.4.13.18 A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um *link*, assim como, permitir definir a quantidade de falhas encontradas no *link* antes de declará-lo inativo, com objetivo de identificar oscilações nos *links*, que possam impactar os serviços e a experiência dos usuários;

4.4.13.19 A solução deve suportar nativamente conectores com clouds públicas, permitindo a extração de metadados dinâmicos para criação de objetos, facilitando a criação de regras de *firewall* e *VPN*;

4.4.13.20 Deve possibilitar a definição de largura de banda distintas nas interfaces para *download* e *upload*;

4.4.13.21 A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (*upload e download*) e nível de qualidade dos links (*perda de pacote, jitter e latência*);

4.4.13.22 Deve implementar balanceamento de *link* por *hash* do *IP* de origem;

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

4.4.13.24 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*;

4.4.13.25 O *appliance* físico deve apresentar compatibilidade com modems *USB (3G/4G)*, onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de *Internet*, e alternativamente, funcionar como circuito *Standby*, onde apenas seja acionado na eventualidade de falha no *link* principal;

4.4.13.26 Deve ser possível extrair informações de desempenho das verificações de saúde mediante *REST API*, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

#### **4.5. SERVIÇO DE GERENCIAMENTO DE EXPOSIÇÃO A AMEAÇAS**

4.5.1 A entidade requer uma solução de inteligência cibernética de ameaças que ajude a fornecer melhor gerenciamento e visibilidade do risco digital nela.

4.5.2 A solução deve coletar inteligência de várias fontes, como *Darkweb, Open Source e Technical Research*.

4.5.3 A inteligência deve ter uma classificação de confiança com base no padrão da indústria, como (Sistema do Almirantado) para todos os relatórios publicados

4.5.4 Todos os relatórios de inteligência devem ser pontuados com base em critérios de relevância específicos para o cenário de ameaças do cliente.

4.5.5 A Inteligência de Ameaças enviada deve abranger todas as ameaças relevantes para o Cliente.

4.5.6 A solução deve monitorar e relatar ameaças em novas vulnerabilidades e explorações que são discutidas ativamente na *Dark Web* e em fontes abertas

4.5.7 A inteligência de ameaças deve ser mapeada para a estrutura *MITRE ATT&CK*

4.5.8 A inteligência deve ser fornecida e atualizada em tempo real à medida que novas informações ou contextos são coletados de várias fontes.

4.5.9 A solução deve fornecer informações sobre vazamentos de credenciais por meio de violações de terceiros em uma visualização limpa da linha do tempo

4.5.10 A solução deve ter uma forte presença em sites da *Darknet* examinados e somente para convidados, como fóruns e mercados.

4.5.11 A solução deve fazer um amplo monitoramento da *Dark Web* para inteligência específica da organização, monitorando salas de bate-papo ocultas, sites privados, redes ponto a ponto, plataforma de mídia social, sites do mercado negro e botnets.

4.5.12 A solução deve fazer a descoberta de dados vazados na *Dark web*, incluindo arquivos confidenciais, dados financeiros/de cartão de crédito, dados pessoais (PII), etc.

4.5.13 A solução deve ser capaz de demonstrar a capacidade de interagir com atores na *Dark Web* e coletar informações por meio do *HUMINT*.

4.5.14 A solução deve ter a capacidade de girar para a inteligência em termos de vários filtros, tais como, no mínimo:

- Nome do adversário,
- Motivação do adversário,
- Indústria de destino,
- Geografia alvo
- Tipos de relatórios,
- Classificações de relevância

4.5.15 A solução deve ter a capacidade de produzir relatórios de alerta precoce com base em ataques iniciais e futuros e novas táticas, técnicas e procedimentos (TTP).

4.5.16 A solução deve ter a capacidade de relatar exclusivamente *Ransomware* e ataques TTP relacionados

4.5.17 A solução deve ter a capacidade de realizar investigação inicial dentro do sistema usando enriquecimentos em tempo real para procurar indicadores de comprometimento (IOCs).

4.5.18 A solução deve ter a capacidade de rastrear e monitorar marcas, assim como:

- 4.5.18.1. Detectar credenciais violadas, ou seja, e-mails. (No caso de clientes do Banco, os dados do Cartão também podem ser incluídos)
- 4.5.18.2. Identificar credenciais vazadas que estão disponíveis na *dark web*
- 4.5.18.3. Identificar a fonte da violação de dados (incluindo terceiros)
- 4.5.18.4. Detectar informações vazadas e dados confidenciais
- 4.5.18.5. Possuir capacidade de monitorar o Cliente como uma marca para quaisquer ataques de *phishing* iminentes
- 4.5.18.6. Fazer a detecção de *sites* de *phishing* através do uso de marcas d'água digitais.
- 4.5.18.7. Identificar o endereço *IP* e *e-mails* de usuários de *phishing* por meio de campanhas de *phishing*
- 4.5.18.8. Ter capacidade de identificar nomes de domínio de aparência semelhante que correspondam ao cliente



- 4.5.19 Serviço de remoção: remoção de conteúdo suspeito (*sites/perfil/etc.*)
- 4.5.20 A solução deve fazer a exposição e varredura de *Shadow IT*: varreduras de portas, dispositivos mal configurados, varreduras de certificados *SSL*, etc.
- 4.5.21 A solução deve ter suporte para categorizar as descobertas de inteligência de ameaças por meio do *MITRE ATT&CK Framework*, etc.
- 4.5.22 solução deve apresentar vulnerabilidades ou configurações incorretas do servidor (nuvem/local)
- 4.5.23 A solução deve ter relatórios de ativos vulneráveis e ativos de sombra de TI
- 4.5.24 A solução deve ter a capacidade de escanear e monitorar a infraestrutura de Internet do Cliente para:
- Identificação de Ativos
  - Identificar a mudança nos ativos da Internet
  - Identificação de Mudanças em Portos Abertos
  - Identifique qualquer certificado *SSL* expirado ou prestes a expirar
- 4.5.25 A solução deve ter as seguintes funcionalidades de gestão:
- Deve ter funções para analisar e investigar indicadores de comprometimento (*IOCs*) sob demanda, como pesquisas de reputação de *IP/Domínio/Hash/CVE* para vários parâmetros, tais como, no mínimo:
  - Informação básica
  - Pesquisa na lista negra
  - Localização geográfica
  - Informações de rede
  - Relatórios de inteligência anteriores
- 4.5.26 A plataforma deve ter recursos para integrar com plataformas de colaboração como *Microsoft Teams* ou *Slack*
- 4.5.27 A plataforma deve ter recursos para fornecer acesso baseado em função, alertas personalizados, alertas *flash*, etc.
- 4.5.28 Deve ter a capacidade de fornecer analista sob demanda para qualquer pesquisa personalizada e requisitos de esclarecimento
- 4.5.29 Você deve dar suporte a segurança adicional fornecendo autenticação de dois fatores para o portal da *web*
- 4.5.30 A solução deve monitorar pessoas importantes da organização (*VIPs*), principalmente em sites de *Doxing*. As redes sociais suportadas deverão ser, no mínimo: *Facebook, Instagram, X (antigo Twitter) e LinkedIn*.

- 4.5.31 A solução deve estar em conformidade com o *MITRE*, mostrando as ameaças e como elas estão localizadas na matriz.
- 4.5.32 A solução deve apresentar uma lista atualizada de agentes de ameaças comuns e palavras-chave *da deep* e *dark web*.
- 4.5.33 A solução deve trazer informações de inteligência sobre *Stealers*, mostrando possíveis funcionários e clientes das organizações infectados por esse tipo de *malware*.
- 4.5.34 A solução deve apresentar uma página *web* com estatísticas de disponibilidade do Portal *Web* da solução.
- 4.5.35 Solução deve oferecer acesso e exportação de informações via *Rest API*.
- 4.5.36 A solução deve oferecer *Logs* de Auditoria, incluindo informações de *logon*.
- 4.5.37 A solução deve permitir que o analista pesquise na *deep* e *darkweb*, incluindo fóruns, *sites* de colagem, aplicativos de mensagens e outras fontes.
- 4.5.38 A solução deverá apresentar, para cada domínio detectado, um relatório de integridade do *DNS*.

## **4.6 Segurança de Infraestrutura como Código (IaC)**

### **4.6.1 Segurança de Infraestrutura como Código (IaC)**

- 4.6.1.1 Detecção automática de vulnerabilidades em templates *IaC*.
- 4.6.1.2 Suporte a múltiplas linguagens *IaC* (ex: *Terraform*, *CloudFormation*).
- 4.6.1.3 Análise de políticas de segurança automatizada para *IaC*.
- 4.6.1.4 Correlação de vulnerabilidades *IaC* com riscos no ambiente.
- 4.6.1.5 Integração das verificações *IaC* no *pipeline CI/CD*.
- 4.6.1.6 Capacidade para bloqueio/enforcement preventivo de códigos não conformes.
- 4.6.1.7 Visualização centralizada de faltas e vulnerabilidades *IaC*.
- 4.6.1.8 Correção automática sugerida para vulnerabilidades *IaC*.
- 4.6.1.9 Análise contínua de segurança de *IaC* com alertas em tempo real.
- 4.6.1.10 Suporte para monitoramento de compliance *IaC* baseado em regras públicas (ex: *CIS Benchmarks*).

### **4.6.2 Segurança de Aplicações (SAST, SCA)**

- 4.6.2.1 Escaneamento de código fonte para detecção de vulnerabilidades (*SAST*).
- 4.6.2.2 Análise de composição de *software* (*SCA*) para identificação de bibliotecas vulneráveis.
- 4.6.2.3 Suporte ao escaneamento automático e manual.

- 4.6.2.4 Identificação de credenciais e segredos expostos no código.
- 4.6.2.5 Correlação de resultados *SAST* com dados em tempo de execução.
- 4.6.2.6 Informações detalhadas para remediação de vulnerabilidades.
- 4.6.2.7 *Dashboards* centralizados para risco de segurança em código.
- 4.6.2.8 Análise em tempo real no pipeline *CI/CD*.
- 4.6.2.9 Relatórios detalhados de vulnerabilidades e riscos de código.
- 4.6.2.10 Funcionalidade para priorização inteligente de vulnerabilidades.

#### **4.6.3 Detecção e Resposta a Vulnerabilidades Ativas e Riscos**

- 4.6.3.1 Monitoramento contínuo para identificar vulnerabilidades ativas em *runtime*.
- 4.6.3.2 Análise de comportamento anômalo do código em execução.
- 4.6.3.3 Alertas compostos correlacionando múltiplos eventos de segurança.
- 4.6.3.4 Detecção de ataques como *ransomware*, comprometimento de credenciais, etc.
- 4.6.3.5 Capacidade de integração para responder automaticamente a ameaças.
- 4.6.3.6 Relatórios e evidências detalhadas para investigação de incidentes.
- 4.6.3.7 Suporte para análise comportamental e inteligência artificial.
- 4.6.3.8 Integração com plataformas de automação para resposta a incidentes.
- 4.6.3.9 Identificação de permissões excessivas em identidades *cloud* (*CIEM*).
- 4.6.3.10 Indicadores de risco baseados em múltiplos fatores de permissão.

#### **4.6.4 Integração e Usabilidade**

- 4.6.4.1 Interface de navegação intuitiva para configuração e análise.
  - 4.6.4.2 Fácil integração com repositórios e ferramentas *CI/CD* populares.
  - 4.6.4.3 Suporte a *workflows DevOps* com alertas acionáveis.
  - 4.6.4.4 Visualização de riscos em múltiplos ambientes de nuvem.
  - 4.6.4.5 Relatórios customizáveis para diferentes perfis (desenvolvedores, admins).
  - 4.6.4.6 Suporte para múltiplos provedores de nuvem (*AWS, Azure, GCP*).
  - 4.6.4.7 Funcionalidade para escalonamento e priorização automática de alertas.
  - 4.6.4.8 Suporte para análise histórica e auditoria de segurança.
  - 4.6.4.9 Suporte para múltiplos perfis de usuário com controle de acesso.
  - 4.6.4.10 Documentação pública e exemplos claros para configuração e uso

## **5. DO MODELO DE EXECUÇÃO DO OBJETO (art. 6º, inciso XXIII, alínea ‘E’ da Lei nº 14.133/2021).**

Para que a solução adquirida produza os resultados pretendidos desde seu início até o encerramento do objeto contratual, é preciso atentar para os aspectos descritos neste item.

O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial (Lei nº 14.133/2021, art. 115, *caput*).

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

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

### **5.1. NÍVEIS MÍNIMOS DE QUALIDADE DE SERVIÇO**

A CONTRATADA, durante toda a vigência contratual, deverá permitir chamados ilimitados para o suporte técnico.

A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio da CONTRATANTE ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da execução demandadas pela contratante.

Todas as atualizações que envolvam indisponibilidade do ambiente, devem ser agendadas previamente com a equipe técnica da CONTRATANTE.

O atendimento técnico tipo “on-site” a ser prestado pelo próprio fabricante do equipamento ou por empresa devidamente treinada e credenciada pelo mesmo, também deverá disponibilizar recurso (Telefone/*website*) para abertura de chamados técnicos em horário 24X7, ou seja, 24 horas por dia e 7 dias por semana, para os equipamentos novos, em garantia.

A CONTRATANTE poderá solicitar a execução de serviço técnico especializado através de canais de comunicação, como:

- *E-mail*;
- Sistema de Chamados *Web*;
- Telefônico.

A CONTRATANTE considerará efetivamente realizado o serviço quando houver confirmação por sua área técnica da conclusão satisfatória do atendimento.

Todas as solicitações técnicas somente poderão ser encerradas com a anuência da CONTRATADA e da CONTRATANTE.

A CONTRATADA manterá cadastro das pessoas indicadas pela CONTRATANTE que poderão efetuar a abertura e fechamento das solicitações de serviço.

O término do atendimento não poderá ultrapassar o prazo estipulado para os diferentes níveis de criticidade.

A CONTRATADA deverá iniciar o atendimento de acordo com os prazos estipulados para o nível de criticidade.

A manutenção e suporte corretivo compreende os serviços de substituição dos equipamentos quando da ocorrência de quaisquer falhas ou defeitos nos componentes de *hardware*, em acordo com a política do fabricante.

O suporte técnico consiste no restabelecimento do funcionamento correto das soluções cobertas por esta contratação, assim como suas funcionalidades, através de um conjunto de ações e atividades (de configuração) que permitam a habilitação, a implementação/aplicação, a manutenção e a colocação em produção de quaisquer funcionalidades destes dispositivos.

Fica facultado à equipe técnica da CONTRATANTE o fornecimento de acesso remoto para atendimento do tipo, em caso em que os problemas identificados permitam esse tipo de atuação.

## 5.2. PRAZOS PARA ATENDIMENTO DE OCORRÊNCIAS

Os níveis de severidade são descritos abaixo:

- Severidade 1 – quando ocorre a perda ou paralisação de serviços relevantes prestados pela CONTRATANTE ou atividades exercidas por ela, configurando-se como emergência;
- Severidade 2 – quando se verifica uma grave perda de funcionalidade, no entanto, sem interromper os serviços prestados pela CONTRATANTE ou atividades exercidas por ela;
- Severidade 3 – quando se verifica uma perda de menor relevância de funcionalidades, causando apenas inconveniências para a devida prestação dos serviços pela CONTRATANTE ou a realização de atividades exercidas por ela;

O nível de severidade será atribuído pela CONTRATANTE no momento da abertura do chamado.

Para os chamados de Suporte Técnico, deverão ser considerados os seguintes prazos de acordo com os níveis de severidade:

<b>Prazos para suporte técnico para ocorrências de hardware e software (a partir do registro da ocorrência)</b>			
Severidade informada	Tempo de Resposta	Tempo diagnostico máximo	Tempo máximo Substituição de Equipamento
1	60 minutos	8 horas corridas	24 horas
2	4 horas	24 horas corridas	48 horas
3	8 horas	48 horas corridas	72 horas

Para fins de cálculo do período decorrido para solução da ocorrência de *software*, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência.

Em caso de substituição definitiva de *hardware*, o equipamento deverá ser novo e original, conforme política do fabricante, com configuração igual ou superior à do equipamento substituído.

Nos casos de substituição definitiva, a CONTRATADA deverá entregar um documento referente à substituição do equipamento antigo pelo equipamento de substituição definitivo (novo). Neste documento deverão constar a descrição e o número de série do equipamento defeituoso e a descrição e o número de série do equipamento novo.

Para fins de cálculo do período decorrido para solução da ocorrência de *hardware*, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência. Nos casos em que houver a substituição do módulo ou equipamento defeituoso para a solução da ocorrência, o seu fechamento efetivo se dará somente após a entrada em operação do novo módulo ou equipamento (de substituição).

### **5.3. SERVIÇO TÉCNICO DE BANCO DE HORAS EM HORÁRIO DE EXPEDIENTE:**

O Banco de Horas para atividades técnicas, pelo período de 12 (doze) meses, será utilizado quando da necessidade de aprimoramento das soluções e demais atividades descritas relativas à solução adquirida.

A realização dos serviços e a quantidade de horas utilizadas serão prévia e formalmente ajustadas entre o TCMSP e a CONTRATADA, as quais serão faturadas pela CONTRATADA no mês seguinte à sua efetiva utilização.

Esse item contempla 250 (duzentas e cinquenta) horas de serviços profissionais a serem executados.

Os serviços técnicos deverão ser executados por equipe certificada da CONTRATADA.

Não serão aceitos profissionais com certificações de nível comercial para execução desses serviços.

Os serviços profissionais em horário de expediente poderão ser executados em horário comercial, entre as 8:00 e as 18:00, de segunda-feira a sexta-feira, exceto em feriados.

Será de responsabilidade da CONTRATADA, antes da execução dos serviços, preparar documento/ata com proposta de quantidade de horas que serão empregadas. O documento formal deverá ser assinado e enviado para a CONTRATANTE. Após a execução dos serviços, a CONTRATANTE irá medir os serviços, conforme a execução observada na prática, justificando eventuais mudanças de quantitativo superiores a 20% do inicialmente planejado.

A CONTRATADA deverá garantir que os serviços objeto atenderão ao padrão de qualidade exigido pela equipe do Núcleo de Tecnologia da Informação.

O serviço deverá ser executado de modo presencial, sempre que requisitado pela CONTRATANTE.

Toda solicitação, via *e-mail* ou contato telefônico, quanto ao consumo das horas deverá ser retornada no prazo máximo de 24 (vinte e quatro) horas após o seu respectivo registro, entendido este retorno como um contato inicial para fins de definição da forma de tratamento da demanda apresentada.

Toda atividade executada deverá ser acompanhada por equipe técnica designada do TCMSP.

#### **5.4. SERVIÇO TÉCNICO DE BANCO DE HORAS EM HORÁRIO EXTRAORDINÁRIO:**

O Banco de Horas para atividades técnicas, pelo período de 12 (doze) meses, será utilizado quando da necessidade de aprimoramento das soluções e demais atividades relativas à solução adquirida.

A realização dos serviços e a quantidade de horas utilizadas serão prévia e formalmente ajustadas entre o TCMSP e a CONTRATADA, as quais serão faturadas pela CONTRATADA, no mês seguinte à sua efetiva utilização.

Esse item contempla 150 (cento e cinquenta) horas de serviços profissionais a serem executados.

Os serviços técnicos deverão ser executados por equipe certificada da CONTRATADA.

Não serão aceitos profissionais com certificações de nível comercial para execução desses serviços.

Os serviços profissionais em horário fora de expediente poderão ser executados em horário extraordinário, entre as 18:00 e as 08:00, de segunda-feira a sexta-feira, e durante qualquer período em finais de semana e feriados.

Será de responsabilidade da CONTRATADA, antes da execução dos serviços, preparar documento/ata com proposta de quantas horas serão empregadas. O documento formal deverá ser assinado e enviado para a CONTRATANTE. Após a execução dos serviços, a CONTRATANTE irá medir os serviços conforme a execução observada, justificando eventuais mudanças de quantitativo superiores a 20% do inicialmente planejado.

A CONTRATADA deverá garantir que os serviços objeto atenderão ao padrão de qualidade exigido pela equipe do Núcleo de Tecnologia da Informação.

O serviço deverá ser executado de modo presencial, sempre que requisitado pela CONTRATANTE.

Toda solicitação, via *e-mail* ou contato telefônico, quanto ao consumo das horas deverá ser retornada no prazo máximo de 24 (vinte e quatro) horas após o seu respectivo registro, entendido este retorno como um contato inicial para fins de definição da forma de tratamento da demanda apresentada.

Toda atividade executada deverá ser acompanhada por equipe técnica designada do TCMSP.



## **5.5. PRAZOS.**

A CONTRATADA deverá entregar, instalar e configurar toda a solução no prazo máximo de 60 (sessenta) dias corridos, a partir da emissão da Ordem de Fornecimento. Atrasos na entrega serão aceitos mediante condições extraordinárias e deverão ser avisados com antecedência máxima de até 15 (quinze) dias corridos prévios ao limite do prazo.

Atrasos na entrega de quaisquer componentes estarão sujeitos a multas e sanções.

O Banco de Horas deverá ser prestado pelo período de 12 (doze) meses, a partir do Termo de Recebimento Provisório.

Os serviços são enquadrados como continuado tendo em vista a necessidade de manutenção da atividade administrativa, decorrente de necessidade prolongada.

O prazo de vigência da contratação por item, relativo aos itens 02, 03, 04, 05, 06, 07, 08, 10 e 11 é passível de renovação dentro dos limites legais, na forma dos arts. 106 e 107 da Lei Federal 14.133/21, mantidas as demais condições da contratação decorrente deste Termo de Referência.

## **6. MODELO DE GESTÃO CONTRATUAL (arts. 6º, XXIII, alínea “f” e art. 117 da Lei nº 14.133/2021).**

O gerenciamento e a fiscalização do contrato caberão ao fiscal e seu substituto, previamente designados pela autoridade competente quando da formalização do ajuste, com atenção às atribuições constantes do art. 117 da Lei Federal nº 14.133/2021.

Ficam reservados ao fiscal do contrato, o direito e a autoridade para resolver todo e qualquer caso singular, omissos ou duvidosos não previstos no processo administrativo e tudo o mais que se relacione com o objeto contratado, desde que não acarrete ônus para a CONTRATANTE ou modificação da contratação.

As decisões que ultrapassarem a competência do fiscal do contrato deverão ser solicitadas formalmente à autoridade administrativa imediatamente superior, em tempo hábil para a adoção de medidas.

## **7. DOS CRITÉRIOS DE MEDIÇÃO E PAGAMENTO (ART. 6º, XXIII, ALÍNEA “G” DA LEI Nº 14.133/2021).**

O pagamento será realizado em uma única vez, em até 30 (trinta) dias corridos contados do recebimento da nota fiscal ou documento equivalente, mediante ateste do responsável pela fiscalização do CONTRATO, dos documentos exigidos em lei ou em CONTRATO, desde que cumpridas todas as exigências legais e contratuais pela CONTRATADA, por meio de depósito em conta corrente ou de ficha de compensação, ambas de titularidade da CONTRATADA.

O Banco de Horas será pago no prazo de até 10 (dez) dias úteis contados do recebimento da nota fiscal ou documento equivalente, mediante ateste do responsável pela fiscalização do CONTRATO e apresentação dos documentos exigidos em lei e no CONTRATO, desde que cumpridas todas as obrigações legais e contratuais pela CONTRATADA. O pagamento será realizado por meio de depósito em conta corrente ou ficha de compensação de titularidade da CONTRATADA.

**8. DA FORMA E DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR (ART. 6º, INCISO XXIII, ALÍNEA 'H', DA LEI Nº 14.133/2021).**

O bem contemplado neste Termo de Referência se enquadra na definição do art. 6º, XIII da Lei nº 14.133/21, pois possuem padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais no mercado.

O fornecedor será selecionado por meio da realização de procedimento licitatório, modalidade Pregão.

O critério de julgamento adotado será o **MENOR PREÇO TOTAL GLOBAL.**

**9. DA ADEQUAÇÃO ORÇAMENTÁRIA (ART. 6º, INCISO XXIII, ALÍNEA 'J', DA LEI Nº 14.133/2021).**

As despesas resultantes do presente instrumento correrão por conta dos recursos constantes das dotações 10.10.01.032.3024.2100.4490.52 – Equipamentos e Material Permanente, 10.10.01.032.3011.2818.3390.40 e 10.10.01.126.3024.2171.3390.40 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica.

**ANEXO II**  
**MODELO DE PROPOSTA COMERCIAL**  
**(A SER PREENCHIDA PELA EMPRESA CLASSIFICADA EM PRIMEIRO LUGAR)**

Ao Tribunal de Contas do Município de São Paulo  
 Endereço: Av. Professor Ascendino Reis 1.130, São Paulo  
 Processo: TC/001321/2026  
 Pregão nº 90.010/2026  
 Abertura dia 17/06/2026 às 9 horas.

A empresa \_\_\_\_\_ CNPJ. nº \_\_\_\_\_, estabelecida na \_\_\_\_\_ nº \_\_\_\_\_, complemento: \_\_\_\_\_, Bairro: \_\_\_\_\_, Cidade: \_\_\_\_\_, Estado: \_\_\_\_\_, telefone: \_\_\_\_\_, e-mail: \_\_\_\_\_, por meio de seu representante legal, Sr.(a) \_\_\_\_\_ (estado civil), \_\_\_\_\_ (profissão), portador(a) do RG nº \_\_\_\_\_ e CPF nº \_\_\_\_\_, observadas as especificações constantes do Anexo I do Edital, propõe o seguinte:

Item	Descrição	Qtde.	Métrica	Período (Meses)	Valor unitário	Valor total
01	<b>FIREWALL DE PRÓXIMA GERAÇÃO:</b> FORTIGATE-201G ou SUPERIOR - 10 X GE RJ45 (INCLUDING 1 X MGMT PORT, 1 X HA PORT, 8 X SWITCH PORTS), 4 X GE SFP SLOTS, 8 X 5GE RJ45, 8 X 10GE SFP+ SLOTS, NP7LITE AND CP10 HARDWARE ACCELERATED, 480GB ONBOARD SSD STORAGE.	2	Equipamento	Entrega única	R\$	R\$
02	FORTIGATE-201G ou SUPERIOR - 3 YEAR ENTERPRISE PROTECTION (IPS, AI-BASED INLINE MALWARE PREVENTION, INLINE CASB DATABASE, DLP, APP CONTROL, ADV MALWARE PROTECTION, URL/DNS/VIDEO FILTERING, ANTI-SPAM, ATTACK SURFACE SECURITY, CONVERTER SVC, FORTICARE PREMIUM).	2	Licença	36	R\$	R\$
03	FORTIGATE-201G OU SUPERIOR - 3 YEAR NEXT CALENDAR DAY DELIVERY PRIORITY RMA SERVICE (REQUIRES FORTICARE PREMIUM OR FORTICARE ELITE).	2	Licença	36	R\$	R\$
04	DATALAKE DE SEGURANÇA: FORTIANALYZER-VM SUBSCRIPTION LICENSE WITH SUPPORT 3 YEAR SUBSCRIPTION LICENSE FOR 5 GB/DAY CENTRAL LOGGING & ANALYTICS. INCLUDE FORTICARE PREMIUM SUPPORT, IOC, SECURITY AUTOMATION SERVICE AND FORTIGUARD OUTBREAK DETECTION SERVICE.	3	Licença	36	R\$	R\$
05	GERENCIADOR DE FIREWALLS: FORTIMANAGER-VM SUBSCRIPTION LICENSE WITH SUPPORT SUBSCRIPTION LICENSE FOR 10 DEVICES/VDOMS MANAGED BY FORTIMANAGER VM S-SERIES 24X7 FORTICARE SUPPORT INCLUDED.	1	Licença	36	R\$	R\$

06	FIREWALL DE PRÓXIMA GERAÇÃO VIRTUAL PARA CLOUD: SUBSCRIPTIONS LICENSE FOR FORTIGATE-VM (2 CPU) WITH ENTERPRISE BUNDLE INCLUDED.	6	Licença	36	R\$	R\$
07	SERVIÇO DE GERENCIAMENTO DE EXPOSIÇÃO A AMEAÇAS: EXTERNAL ATTACK SURFACE MONITORING, BRAND PROTECT & ADVERSARY CENTRIC INTELLIGENCE - UP TO 500 MONITORED ASSETS. FORTICARE PREMIUM SUPPORT INCLUDED 1 YEAR SUBSCRIPTION.	1	Licença	12	R\$	R\$
08	SOLUÇÃO DE SEGURANÇA PARA DESENVOLVIMENTO DE APLICAÇÕES: LACEWORK CODE SECURITY FOR 1 CODE CONTRIBUTING DEVELOPER (MINIMUM ORDER QUANTITY 20 DEVELOPERS), INCLUDES FORTICARE PREMIUM. 1 YEAR SUBSCRIPTION.	20	Licença	12	R\$	R\$
09	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	1	Serviço	Entrega Única	R\$	R\$
10	SUORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, NOS DIAS ÚTEIS ENTRE 8H E 18H	250	Hora	12	R\$	R\$
11	SUORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, EM DIAS NÃO ÚTEIS	150	Hora	12	R\$	R\$

**Valor total geral (em algarismos e por extenso)**

VALIDADE DA PROPOSTA: Será de \_\_\_\_\_ dias contados a partir da data de abertura da Sessão Pública (mínimo de 60 dias).

CONDIÇÕES DE PAGAMENTO: conforme Anexo V - Minuta de Contrato.

INFORMAÇÕES PARA PAGAMENTO: banco\_\_\_\_, número da conta \_\_\_\_\_ e agência \_\_\_\_.

DECLARA, para todos os fins:

- estar apta e/ou autorizada pela fabricante a comercializar e a prestar suporte técnico da solução objeto do certame.
- que os produtos fornecidos serão novos, de primeiro uso, em linha de fabricação, e
- que os serviços técnicos especializados serão executados por profissionais habilitados e capacitados, detentores de certificados técnicos emitidos pelo fabricante.

[Local], \_\_\_\_ de \_\_\_\_\_ de 2026.

\_\_\_\_\_  
(Assinatura do responsável da proponente)  
NOME:/RG -----

**ANEXO III**  
**MODELO DE DECLARAÇÃO DE ME/EPP E INEXISTÊNCIA DE FATOS SUPERVENIENTES**

Processo: TC/001321/2026  
PREGÃO nº 90.010/2026

A empresa ....., inscrita no CNPJ sob nº....., por intermédio de seu representante legal infra-assinado, Sr(a). .....portador(a) da Carteira de Identidade nº..... e do CPF nº ....., **DECLARA**, sob as penas do artigo 299 do Código Penal que:

I – Se enquadra na condição de **Microempresa (ME)** ou **Empresa de Pequeno Porte (EPP)**, nos termos do artigo 3º da Lei Complementar nº 123/2006;

II – Não incorre em nenhuma das vedações previstas no § 4º do artigo 3º da referida Lei, especialmente aquelas relacionadas à participação societária, faturamento, natureza jurídica e atividades impeditivas;

III – Inexistem fatos supervenientes que conduzam ao seu desenquadramento da condição de ME ou EPP.

[Local], \_\_\_\_ de \_\_\_\_\_ de 2026.

\_\_\_\_\_  
Assinatura do responsável pela empresa proponente

Nome legível: \_\_\_\_\_

RG: \_\_\_\_\_

Cargo: \_\_\_\_\_

Empresa: \_\_\_\_\_

**Obs. A declaração de ME/EPP deverá ser apresentada, SE CABÍVEL, com os documentos de HABILITAÇÃO (subitem 8.14.1 do Edital).**

**ANEXO IV**  
**MODELO DE DECLARAÇÕES**

Processo: TC/001321/2026  
PREGÃO nº 90.010/2026

A empresa ....., inscrita no CNPJ sob nº....., por intermédio de seu representante legal infra-assinado, Sr(a). .....portador(a) da Carteira de Identidade nº..... e do CPF nº ....., **DECLARA** que:

1. Está apta ou devidamente autorizada pelo fabricante da solução objeto do certame a comercializar, implantar e prestar suporte técnico à solução ofertada, em conformidade com as especificações e condições estabelecidas no Edital e em seus anexos.

1.1. Essa condição poderá ser comprovada, a critério exclusivo do licitante, pela presente declaração ou, alternativamente, mediante carta ou certificado emitido pelo fabricante, contrato de distribuição, ou ainda por comprovação em domínio público (site oficial do fabricante da oferta).

2. Compromete-se a manter, durante toda a vigência contratual, profissionais qualificados e aptos à adequada execução do objeto, responsabilizando-se integralmente pela qualidade dos serviços prestados.

Declara, por fim, que todas as informações acima são verdadeiras, estando ciente de que a prestação de informações falsas ou inexatas poderá ensejar a aplicação das sanções administrativas, civis e penais cabíveis, nos termos da legislação vigente.

[Local], \_\_\_\_ de \_\_\_\_\_ de 2026.

\_\_\_\_\_  
Assinatura do responsável pela empresa proponente

Nome legível: \_\_\_\_\_

RG: \_\_\_\_\_

Cargo: \_\_\_\_\_

Empresa: \_\_\_\_\_

**Obs. A declaração de ME/EPP deverá ser apresentada com os documentos de HABILITAÇÃO (subitem 8.14.2 do Edital).**

**ANEXO V**  
**MINUTA DE CONTRATO**

CONTRATO Nº:  
CONTRATANTE: **TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO**  
CONTRATADA: **<DENOMINAÇÃO SOCIAL EMPRESA>**  
OBJETO DO CONTRATO: Contratação de solução tecnológica de segurança da informação, composta por hardware, software e serviços especializados, para fortalecimento da infraestrutura de cibersegurança do TCMSP, incluindo fornecimento de equipamentos FortiGate 201G ou superior e componentes integrados, serviços de suporte, instalação, configuração, manutenção e banco de horas técnicas, conforme especificações e quantitativos previstos no Termo de Referência.  
VALOR: **<R\$ \_\_\_\_\_>**  
DOTAÇÃO(ÕES): **<\_\_\_\_\_>**  
PROCESSO Nº: TC/001321/2026

**O TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO - TCMSP**, CNPJ nº 50.176.270/0001-26, com endereço na Av. Professor Ascendino Reis nº 1.130 – São Paulo - SP, neste ato representado por seu Presidente, **DOMINGOS DISSEI**, doravante denominado **CONTRATANTE**, e **<DENOMINAÇÃO SOCIAL DA EMPRESA>**, CNPJ nº **<\_\_\_\_\_>**, com endereço na **<endereço completo da empresa>**, doravante denominada **CONTRATADA**, neste ato representada por seu **<cargo do representante>**, **<NOME DO REPRESENTANTE>**, resolvem celebrar este CONTRATO, decorrente da licitação na modalidade PREGÃO ELETRÔNICO nº **\_\_\_/\_\_\_\_**, conforme o Edital de Licitação, seus Anexos e a proposta formulada pela **CONTRATADA**, integrantes desta, para todos os efeitos, bem como as seguintes cláusulas:

**CLÁUSULA PRIMEIRA – OBJETO**

1.1. O objeto do presente instrumento é a contratação de solução tecnológica de segurança da informação, composta por hardware, software e serviços especializados, para fortalecimento da infraestrutura de cibersegurança do TCMSP, incluindo fornecimento de equipamentos FortiGate 201G ou superior e componentes integrados, serviços de suporte, instalação, configuração, manutenção e banco de horas técnicas, conforme especificações e quantitativos previstos no Termo de Referência.

1.2. Os produtos abrangidos por esta contratação estão detalhados abaixo:



Item	Descrição	Qtde	Métrica
01	FIREWALL DE PRÓXIMA GERAÇÃO: FORTIGATE-201G ou SUPERIOR - 10 X GE RJ45 (INCLUDING 1 X MGMT PORT, 1 X HA PORT, 8 X SWITCH PORTS), 4 X GE SFP SLOTS, 8 X 5GE RJ45, 8 X 10GE SFP+ SLOTS, NP7LITE AND CP10 HARDWARE ACCELERATED, 480GB ONBOARD SSD STORAGE	2	Equipamento
02	FORTIGATE-201G ou SUPERIOR - 3 YEAR ENTERPRISE PROTECTION (IPS, AI-BASED INLINE MALWARE PREVENTION, INLINE CASB DATABASE, DLP, APP CONTROL, ADV MALWARE PROTECTION, URL/DNS/VIDEO FILTERING, ANTI-SPAM, ATTACK SURFACE SECURITY, CONVERTER SVC, FORTICARE PREMIUM)	2	Licença
03	FORTIGATE-201G OU SUPERIOR - 3 YEAR NEXT CALENDAR DAY DELIVERY PRIORITY RMA SERVICE (REQUIRES FORTICARE PREMIUM OR FORTICARE ELITE)	2	Licença
04	DATALAKE DE SEGURANÇA: FORTIANALYZER-VM SUBSCRIPTION LICENSE WITH SUPPORT 3 YEAR SUBSCRIPTION LICENSE FOR 5 GB/DAY CENTRAL LOGGING & ANALYTICS. INCLUDE FORTICARE PREMIUM SUPPORT, IOC, SECURITY AUTOMATION SERVICE AND FORTIGUARD OUTBREAK DETECTION SERVICE	3	Licença
05	GERENCIADOR DE FIREWALLS: FORTIMANAGER-VM SUBSCRIPTION LICENSE WITH SUPPORT SUBSCRIPTION LICENSE FOR 10 DEVICES/VDOMS MANAGED BY FORTIMANAGER VM S-SERIES 24X7 FORTICARE SUPPORT INCLUDED	1	Licença
06	FIREWALL DE PRÓXIMA GERAÇÃO VIRTUAL PARA CLOUD: SUBSCRIPTIONS LICENSE FOR FORTIGATE-VM (2 CPU) WITH ENTERPRISE BUNDLE INCLUDED	6	Licença
07	SERVIÇO DE GERENCIAMENTO DE EXPOSIÇÃO A AMEAÇAS: EXTERNAL ATTACK SURFACE MONITORING, BRAND PROTECT & ADVERSARY CENTRIC INTELLIGENCE - UP TO 500 MONITORED ASSETS. FORTICARE PREMIUM SUPPORT INCLUDED 1 YEAR SUBSCRIPTION	1	Licença
08	SOLUÇÃO DE SEGURANÇA PARA DESENVOLVIMENTO DE APLICAÇÕES: LACEWORK CODE SECURITY FOR 1 CODE CONTRIBUTING DEVELOPER (MINIMUM ORDER QUANTITY 20 DEVELOPERS), INCLUDES FORTICARE PREMIUM. 1 YEAR 1SUBSCRIPTION.	20	Licença
09	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	1	Serviço
10	SUPORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, NOS DIAS ÚTEIS ENTRE 8H E 18H	250	Hora
11	SUPORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, NOS EM DIAS NÃO ÚTEIS	150	Hora

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. A proposta da **CONTRATADA**;

1.3.3. Demais documentos que instruem esta contratação e anexos dos documentos supracitados.

## CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

**2.1.** O presente CONTRATO é celebrado sob o regime de fornecimento e prestação de serviço associado, nos termos do art. 113 da Lei Federal nº 14.133/2021, e terá sua vigência definida pela soma:

**2.1.1.** do prazo relativo ao fornecimento inicial do objeto, compreendendo a entrega, instalação, configuração e disponibilização da solução contratada; e

**2.1.2.** do prazo relativo aos serviços associados vinculados à solução, inclusive suporte, manutenção, subscrições/licenças e banco de horas, conforme aplicável a cada item.

**2.2.** Os prazos de execução de cada item, bem como seus respectivos marcos iniciais, são os constantes do quadro desta cláusula, devendo ser interpretados em consonância com o regime previsto no art. 113 da Lei Federal nº 14.133/2021 e com o respectivo marco (termo) inicial.

Item	Descrição	Qtde	Métrica	Prazo de execução	Marco (termo) Inicial
01	FIREWALL DE PRÓXIMA GERAÇÃO: FORTIGATE-201G ou SUPERIOR - 10 X GE RJ45 (INCLUDING 1 X MGMT PORT, 1 X HA PORT, 8 X SWITCH PORTS), 4 X GE SFP SLOTS, 8 X 5GE RJ45, 8 X 10GE SFP+ SLOTS, NP7LITE AND CP10 HARDWARE ACCELERATED, 480GB ONBOARD SSD STORAGE	2	Equipamento	Até 60 dias corridos. Entrega única	Emissão da Ordem de Fornecimento
02	FORTIGATE-201G ou SUPERIOR - 3 YEAR ENTERPRISE PROTECTION (IPS, AI-BASED INLINE MALWARE PREVENTION, INLINE CASB DATABASE, DLP, APP CONTROL, ADV MALWARE PROTECTION, URL/DNS/VIDEO FILTERING, ANTI-SPAM, ATTACK SURFACE SECURITY, CONVERTER SVC, FORTICARE PREMIUM)	2	Licença	36 meses	Emissão da Ordem de Início dos Serviços
03	FORTIGATE-201G OU SUPERIOR - 3 YEAR NEXT CALENDAR DAY DELIVERY PRIORITY RMA SERVICE (REQUIRES FORTICARE PREMIUM OR FORTICARE ELITE)	2	Licença	36 meses	Emissão da Ordem de Início dos Serviços
04	DATALAKE DE SEGURANÇA: FORTIANALYZER-VM SUBSCRIPTION LICENSE WITH SUPPORT 3 YEAR SUBSCRIPTION LICENSE FOR 5 GB/DAY CENTRAL LOGGING & ANALYTICS. INCLUDE FORTICARE PREMIUM SUPPORT, IOC, SECURITY AUTOMATION SERVICE AND FORTIGUARD OUTBREAK DETECTION SERVICE	3	Licença	36 meses	Emissão da Ordem de Início dos Serviços

05	GERENCIADOR DE FIREWALLS: FORTIMANAGER-VM SUBSCRIPTION LICENSE WITH SUPPORT SUBSCRIPTION LICENSE FOR 10 DEVICES/VDOMS MANAGED BY FORTIMANAGER VM S-SERIES 24X7 FORTICARE SUPPORT INCLUDED	1	Licença	36 meses	Emissão da Ordem de Início dos Serviços
06	FIREWALL DE PRÓXIMA GERAÇÃO VIRTUAL PARA CLOUD: SUBSCRIPTIONS LICENSE FOR FORTIGATE-VM (2 CPU) WITH ENTERPRISE BUNDLE INCLUDED	6	Licença	36 meses	Emissão da Ordem de Início dos Serviços
07	SERVIÇO DE GERENCIAMENTO DE EXPOSIÇÃO A AMEAÇAS: EXTERNAL ATTACK SURFACE MONITORING, BRAND PROTECT & ADVERSARY CENTRIC INTELLIGENCE - UP TO 500 MONITORED ASSETS. FORTICARE PREMIUM SUPPORT INCLUDED 1 YEAR SUBSCRIPTION	1	Licença	12 meses	Emissão da Ordem de Início dos Serviços
08	SOLUÇÃO DE SEGURANÇA PARA DESENVOLVIMENTO DE APLICAÇÕES: LACEWORK CODE SECURITY FOR 1 CODE CONTRIBUTING DEVELOPER (MINIMUM ORDER QUANTITY 20 DEVELOPERS), INCLUDES FORTICARE PREMIUM. 1 YEAR 1SUBSCRIPTION.	20	Licença	12 meses	Emissão da Ordem de Início dos Serviços
09	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	1	Serviço	Até 60 dias corridos. Entrega única	Emissão da Ordem de Fornecimento
10	SUPORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, NOS DIAS ÚTEIS ENTRE 8H E 18H	250	Hora	12 meses	Emissão do Termo de Recebimento Provisório dos itens 01 e 09
11	SUPORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, NOS EM DIAS NÃO ÚTEIS	150	Hora	12 meses	Emissão do Termo de Recebimento Provisório dos itens 01 e 09

### 2.3. A Ordem de Fornecimento e a Ordem de Início dos Serviços será emitida em data a ser definida pelo CONTRATANTE.

**2.3.1.** O envio das Ordem de Fornecimento e Ordem de Início dos Serviços se dará de forma eletrônica (e-mail), com prazo de 2 (dois) dias úteis para confirmação do recebimento do e-mail. Transcorrido o referido prazo sem manifestação expressa da **CONTRATADA**, considerar-se-á que a Ordem de Fornecimento e a Ordem de Início de Serviços foram devidamente recebidas.

**2.4.** A **CONTRATADA** deverá entregar, instalar e configurar toda a solução no prazo máximo de 60 (sessenta) dias corridos, a partir da emissão da Ordem de Fornecimento.

**2.5.** Atrasos na entrega serão aceitos mediante condições extraordinárias e deverão ser avisados com antecedência máxima de até 15 (quinze) dias corridos prévios ao limite do prazo.

**2.6.** Atrasos na entrega de quaisquer componentes estarão sujeitos a multas e sanções previstas neste CONTRATO.

**2.7.** O Banco de Horas deverá ser prestado pelo período de 12 (doze) meses, a partir da emissão da Ordem de Início dos Serviços.

**2.8.** O prazo de vigência da contratação dos itens 02, 03, 04, 05, 06, 07, 08, 10 e 11 são passíveis de prorrogação dentro dos limites legais, na forma dos arts. 106 e 107 da Lei Federal nº 14.133/2021.

**2.9.** Para registrar os marcos iniciais mencionados no quadro da subcláusula 2.2, o responsável pela fiscalização do CONTRATO deverá emitir documento com as respectivas datas, que será anexado aos autos desta contratação.

**2.10.** A prorrogação de CONTRATO deverá ser promovida mediante celebração de termo aditivo.

**2.11.** A prorrogação é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para o **CONTRATANTE**, permitida a negociação com a **CONTRATADA**, atentando, ainda, para o cumprimento dos seguintes requisitos:

**2.11.1.** Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

**2.11.2.** Seja juntado relatório que discorra sobre a execução do CONTRATO, com informações de que os serviços tenham sido prestados regularmente;

**2.11.3.** Seja juntada justificativa e motivo, por escrito, de que o **CONTRATANTE** mantém interesse na realização do serviço;

**2.11.4.** Haja manifestação expressa da **CONTRATADA** informando o interesse na prorrogação;

**2.11.5.** Seja comprovado que a **CONTRATADA** mantém as condições iniciais de habilitação; e

**2.11.6.** Não haja registro no CADIN de créditos não quitados do setor público municipal.

**2.12.** A **CONTRATADA** não tem direito subjetivo à prorrogação contratual.

**2.13.** Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

**2.14.** O CONTRATO não poderá ser prorrogado quando a **CONTRATADA** tiver sido penalizada nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

### CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO DO OBJETO E GESTÃO DO CONTRATO

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

### CLÁUSULA QUARTA – SUBCONTRATAÇÃO

**4.1.** É vedada à **CONTRATADA** a subcontratação total ou parcial do objeto deste CONTRATO.

### CLÁUSULA QUINTA – PREÇO

**5.1.** O valor total da contratação é de R\$ <\_\_\_\_\_> (<valor por extenso>), discriminado abaixo:

Item	Descrição	Qtde	Métrica	Prazo de execução	Valor Unitário (R\$)	Valor Total (R\$)
01	FIREWALL DE PRÓXIMA GERAÇÃO: FORTIGATE-201G ou SUPERIOR - 10 X GE RJ45 (INCLUDING 1 X MGMT PORT, 1 X HA PORT, 8 X SWITCH PORTS), 4 X GE SFP SLOTS, 8 X 5GE RJ45, 8 X 10GE SFP+ SLOTS, NP7LITE AND CP10 HARDWARE ACCELERATED, 480GB ONBOARD SSD STORAGE	2	Equipamento	Entrega única		
02	FORTIGATE-201G ou SUPERIOR - 3 YEAR ENTERPRISE PROTECTION (IPS, AI-BASED INLINE MALWARE PREVENTION, INLINE CASB DATABASE, DLP, APP CONTROL, ADV MALWARE PROTECTION, URL/DNS/VIDEO FILTERING, ANTI-SPAM, ATTACK SURFACE SECURITY, CONVERTER SVC, FORTICARE PREMIUM)	2	Licença	36 meses		
03	FORTIGATE-201G OU SUPERIOR - 3 YEAR NEXT CALENDAR DAY DELIVERY PRIORITY RMA SERVICE (REQUIRES FORTICARE PREMIUM OR FORTICARE ELITE)	2	Licença	36 meses		
04	DATALAKE DE SEGURANÇA: FORTIANALYZER-VM SUBSCRIPTION LICENSE WITH SUPPORT 3 YEAR SUBSCRIPTION LICENSE FOR 5 GB/DAY CENTRAL LOGGING & ANALYTICS. INCLUDE FORTICARE PREMIUM SUPPORT, IOC, SECURITY AUTOMATION SERVICE AND FORTIGUARD OUTBREAK DETECTION SERVICE	3	Licença	36 meses		

05	GERENCIADOR DE FIREWALLS: FORTIMANAGER-VM SUBSCRIPTION LICENSE WITH SUPPORT SUBSCRIPTION LICENSE FOR 10 DEVICES/VDOMS MANAGED BY FORTIMANAGER VM S-SERIES 24X7 FORTICARE SUPPORT INCLUDED	1	Licença	36 meses		
06	FIREWALL DE PRÓXIMA GERAÇÃO VIRTUAL PARA CLOUD: SUBSCRIPTIONS LICENSE FOR FORTIGATE-VM (2 CPU) WITH ENTERPRISE BUNDLE INCLUDED	6	Licença	36 meses		
07	SERVIÇO DE GERENCIAMENTO DE EXPOSIÇÃO A AMEAÇAS: EXTERNAL ATTACK SURFACE MONITORING, BRAND PROTECT & ADVERSARY CENTRIC INTELLIGENCE - UP TO 500 MONITORED ASSETS. FORTICARE PREMIUM SUPPORT INCLUDED 1 YEAR SUBSCRIPTION	1	Licença	12 meses		
08	SOLUÇÃO DE SEGURANÇA PARA DESENVOLVIMENTO DE APLICAÇÕES: LACEWORK CODE SECURITY FOR 1 CODE CONTRIBUTING DEVELOPER (MINIMUM ORDER QUANTITY 20 DEVELOPERS), INCLUDES FORTICARE PREMIUM. 1 YEAR 1SUBSCRIPTION.	20	Licença	12 meses		
09	SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO	1	Serviço	Entrega única		
10	SUPORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, NOS DIAS ÚTEIS ENTRE 8H E 18H	250	Hora	12 meses		
11	SUPORTE CORRETIVO, NA MODALIDADE BANCO DE HORAS, NOS EM DIAS NÃO ÚTEIS	150	Hora	12 meses		

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

#### CLÁUSULA SEXTA – CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

**6.1.** Os critérios de medição, bem como as demais condições a eles referentes encontram-se definidos no Termo de Referência, anexo a este CONTRATO.

**6.2.** O pagamento referente aos itens de 01 a 09 será efetuado em parcela única, no prazo de até 30 (trinta) dias corridos contados do recebimento da nota fiscal ou documento equivalente, mediante ateste do responsável pela fiscalização do CONTRATO, dos documentos exigidos em lei ou em CONTRATO, desde

que cumpridas todas as exigências legais e contratuais pela **CONTRATADA**, por meio de depósito em conta corrente ou de ficha de compensação, ambas de titularidade da **CONTRATADA**.

**6.3.** O pagamento referente aos itens 10 e 11 será realizado em até 10 (dez) dias úteis contados do recebimento da nota fiscal ou documento equivalente, mediante ateste do responsável pela fiscalização do CONTRATO, dos documentos exigidos em lei ou em CONTRATO, desde que cumpridas todas as exigências legais e contratuais pela **CONTRATADA**, por meio de depósito em conta corrente ou de ficha de compensação, ambas de titularidade da **CONTRATADA**.

**6.4.** Antes dos pagamentos, o **CONTRATANTE** efetuará consulta ao Cadastro Informativo Municipal – CADIN. A existência de registro no CADIN impede a realização de pagamento, conforme estabelecido no inciso II, art. 3º, da Lei Municipal nº 14.094/2005.

**6.5.** Na hipótese de erro ou divergência com as condições contratadas, a nota fiscal ou documento equivalente será recusada pelo **CONTRATANTE**, mediante declaração expressa das razões da desconformidade, ficando estabelecido que o prazo para pagamento será contado a partir da data da apresentação da nova nota fiscal ou documento equivalente, devidamente corrigida.

**6.6.** Os pagamentos efetuados com atraso, por culpa exclusiva do **CONTRATANTE**, terão o valor do principal corrigido monetariamente pelo índice de remuneração básica da caderneta de poupança e incidência de juros simples, no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% “*pro-rata tempore*”), observando-se, para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorrer (conforme Portaria nº 05/2012-SF).

#### **CLÁUSULA SÉTIMA - REAJUSTE**

**7.1.** Os preços serão reajustados aplicando-se o índice IPC-FIPE (mês de referência \_\_\_\_/\_\_\_\_), acumulado em 12 (doze) meses, contados da data do orçamento estimado (\_\_\_\_/\_\_\_\_/\_\_\_\_) e, caso ocorram novas prorrogações, os reajustes subsequentes ao primeiro serão contados da data de início dos efeitos financeiros do último reajuste ocorrido, acumulado em 12 (doze) meses.

**7.2.** A **CONTRATADA** deverá, caso seja solicitado pelo **CONTRATANTE**, instruir o pedido de reajuste com a documentação pertinente, para conferência e para homologação dos cálculos pelo **CONTRATANTE**.

**7.3.** O reajuste terá seus efeitos financeiros iniciados a partir da data de aquisição do direito da **CONTRATADA**, nos termos da subcláusula 7.1.

**7.4.** Na hipótese de divergência de valores entre o apresentado pela **CONTRATADA** e o conferido pelo **CONTRATANTE**, prevalecerá o verificado pelo **CONTRATANTE**, até que as partes dirimam a controvérsia.

**7.5.** O reajuste concedido será registrado por meio de apostila.

#### **CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE**

**8.1.** São obrigações do **CONTRATANTE**:



- 8.1.1.** Exigir, da **CONTRATADA**, o cumprimento de todas as obrigações descritas no Termo de Referência, no CONTRATO, bem como nos demais documentos vinculantes à execução do objeto desta contratação e seus anexos;
- 8.1.2.** Receber o objeto no prazo e condições estabelecidas no Termo de Referência, bem como no artigo 140 da Lei Federal nº 14.133/2021 e nos artigos 140 e 141 do Decreto Municipal nº 62.100/2022;
- 8.1.3.** Notificar a **CONTRATADA**, por escrito, sobre vícios, defeitos, incorreções, imperfeições, falhas ou irregularidades verificadas na execução do objeto contratual, fixando prazo para que seja substituído, reparado ou corrigido, total ou parcialmente, às suas expensas, certificando-se de que as soluções por ela propostas sejam as mais adequadas;
- 8.1.4.** Acompanhar e fiscalizar a execução do CONTRATO e o cumprimento das obrigações pela **CONTRATADA**;
- 8.1.5.** Comunicar a **CONTRATADA** para emissão de nota fiscal ou documento equivalente relativa à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à qualidade e quantidade, conforme o artigo 143 da Lei Federal nº 14.133/2021;
- 8.1.6.** Efetuar o pagamento à **CONTRATADA** do valor correspondente à execução do objeto no prazo, forma e condições estabelecidos no presente CONTRATO e no Termo de Referência;
- 8.1.7.** Aplicar à **CONTRATADA** as sanções previstas na lei e neste CONTRATO;
- 8.1.8.** Não praticar atos de ingerência na administração da **CONTRATADA**;
- 8.1.9.** Cientificar os setores competentes para a adoção das medidas cabíveis quando do descumprimento de obrigações pela **CONTRATADA**;
- 8.1.10.** Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente CONTRATO, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.
- 8.2.** O **CONTRATANTE** não responderá por quaisquer compromissos assumidos pela **CONTRATADA** com terceiros, ainda que vinculados à execução do CONTRATO, bem como por qualquer dano causado a terceiros em decorrência de ato da **CONTRATADA**, de seus empregados, prepostos ou subordinados.

#### **CLÁUSULA NONA - OBRIGAÇÕES DA CONTRATADA**

- 9.1.** A **CONTRATADA** deve cumprir todas as obrigações constantes do Termo de Referência, de sua proposta, deste CONTRATO e de eventuais anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas.
- 9.2.** Atender às determinações regulares emitidas pelo fiscal ou gestor do CONTRATO ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados.
- 9.3.** Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado ao **CONTRATANTE** ou terceiros, não reduzindo essa responsabilidade a

fiscalização ou o acompanhamento da execução contratual pelo **CONTRATANTE**, que ficará autorizado a descontar dos pagamentos devidos o valor correspondente aos danos sofridos.

**9.4.** Manter atualizadas, durante a vigência da contratação, todas as condições de habilitação e qualificação exigidas para esta contratação, compreendendo seus dados cadastrais.

**9.5.** Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo CONTRATO, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao **CONTRATANTE** e não poderá onerar o objeto do CONTRATO.

**9.6.** Paralisar, por determinação do **CONTRATANTE**, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

**9.7.** Manter, durante toda a vigência do CONTRATO, em compatibilidade com as obrigações assumidas, todas as condições exigidas para qualificação na contratação.

**9.8.** Prestar todo e qualquer esclarecimento ou informação que for solicitado pela fiscalização do CONTRATO.

**9.9.** Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do CONTRATO.

**9.10.** Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no artigo 124, inciso II, alínea d, da Lei Federal nº 14.133/2021.

**9.11.** Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do **CONTRATANTE**.

**9.12.** Alocar os empregados e recursos necessários ao perfeito cumprimento das cláusulas deste CONTRATO, com habilitação e conhecimento adequados.

**9.13.** Prestar os serviços dentro dos parâmetros e rotinas estabelecidos.

**9.14.** Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos.

**9.15.** Submeter previamente, por escrito, ao **CONTRATANTE**, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações referentes a esta contratação.

**9.16.** Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho.

**9.17.** Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho.

**9.18.** Manter preposto aceito pelo **CONTRATANTE** para representá-la na execução do CONTRATO.

**9.18.1.** A indicação ou a manutenção do preposto da **CONTRATADA** poderá ser recusada pelo **CONTRATANTE**, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

**9.19.** Não contratar, durante a vigência do CONTRATO, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do **CONTRATANTE** ou de agente público que tenha desempenhado função na contratação direta ou que atue na fiscalização ou gestão do CONTRATO, nos termos do artigo 48, parágrafo único, da Lei Federal nº 14.133/2021.

**9.20.** Prestar todo esclarecimento ou informação solicitada pelo **CONTRATANTE** ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do CONTRATO.

**9.21.** Assegurar aos seus trabalhadores ambiente de trabalho e instalações em condições adequadas ao cumprimento das normas de saúde, segurança e bem-estar no trabalho.

**9.22.** Garantir o acesso do **CONTRATANTE**, a qualquer tempo, aos documentos relativos à execução do CONTRATO.

**9.23.** Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o Termo de Referência e aos demais documentos que informam esta contratação, no prazo determinado.

**9.24.** Instruir seus empregados quanto à necessidade de acatar as normas internas do **CONTRATANTE**.

**9.25.** Responsabilizar-se por quaisquer ações judiciais, reivindicações ou reclamações, sendo a **CONTRATADA** considerada como única e exclusiva responsável por todos os ônus com que o **CONTRATANTE** venha a arcar, em qualquer época, decorrentes de tais ações oriundas do objeto do presente CONTRATO.

#### **CLÁUSULA DÉCIMA- OBRIGAÇÕES PERTINENTES À LGPD**

**10.1.** O uso de dados, informações e conteúdo eventualmente oriundos dos serviços contratados está limitado à finalidade da prestação do objeto, sendo vedado seu uso para finalidades diferentes da expressamente determinada neste documento, sem o prévio consentimento do **CONTRATANTE**, não podendo os dados serem tratados posteriormente de forma incompatível com essa finalidade, incluindo operações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração dos dados.

**10.1.1.** As políticas de proteção de dados pessoais estabelecidas pelo **CONTRATANTE** e as previsões da Lei Geral de Proteção de Dados – LGPD prevalecerão sobre quaisquer disposições eventualmente diversas no presente CONTRATO e demais documentos que instruem este procedimento

**10.2.** A **CONTRATADA** deverá prestar esclarecimentos ao **CONTRATANTE**, sobre eventuais atos ou fatos noticiados que se refiram ao tema desta cláusula.

#### **CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO**

**11.1.** Não haverá exigência de garantia contratual da execução.

## **CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS**

**12.1.** Comete infração administrativa, nos termos da Lei Federal nº 14.133/2021, a **CONTRATADA** que:

- a) Der causa à inexecução parcial do CONTRATO;
- b) Der causa à inexecução parcial do CONTRATO que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) Der causa à inexecução total do CONTRATO;
- d) Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) Apresentar documentação falsa ou prestar declaração falsa durante a execução do CONTRATO;
- f) Praticar ato fraudulento na execução do CONTRATO;
- g) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) Praticar ato lesivo previsto no artigo 5º da Lei Federal nº 12.846/2013.

**12.2.** O cometimento destas ou de qualquer outra infração prevista em lei, condizente com a execução contratual, sujeitará a **CONTRATADA** à aplicação das penalidades descritas nesta cláusula décima segunda.

**12.3.** Serão aplicadas à **CONTRATADA** que incorrer nas infrações acima descritas as seguintes sanções:

**12.3.1.** Advertência, quando a **CONTRATADA** der causa à inexecução parcial do CONTRATO, sempre que não se justificar a imposição de penalidade mais grave;

**12.3.2.** Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” da subcláusula 12.1, sempre que não se justificar a imposição de penalidade mais grave;

**12.3.3.** Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” da subcláusula 12.1, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

**12.3.4.** Multa:

**12.3.4.1.** Moratória, para as infrações descritas no item “d” da subcláusula 12.1, de 1% (um por cento) por dia de atraso injustificado sobre o valor total da contratação, até o limite de 10 (dez) dias corridos.

**12.3.4.2.** Compensatória, para as infrações descritas nas alíneas “e” a “h” da subcláusula 12.1, de 5% (cinco por cento) a 15% (quinze por cento) do valor total da contratação.

**12.3.4.3.** Compensatória, para a infração descrita na alínea “b” da subcláusula 12.1, de 12% (doze por cento) a 15% (quinze por cento) do valor total da contratação.

**12.3.4.4.** Compensatória, para a inexecução total do CONTRATO prevista na alínea “c” da subcláusula 12.1, de 15% (quinze por cento) do valor total da contratação.

**12.3.4.5.** Compensatória, para a infração descrita na alínea “a” da subcláusula 12.1, de 10% (dez por cento) do valor total da contratação.

**12.3.4.6.** Compensatória, por hora de atraso no atendimento aos chamados descritos no Termo de Referência, de 0,5% (meio por cento) sobre o valor total da contratação.

**12.3.4.6.1.** O valor poderá ser majorado para 0,7% sobre o valor da contratação em caso de reincidência num período de 12 (doze) meses.

**12.3.4.7.** Compensatória, de 1% (um por cento), por ocorrência que caracterize o descumprimento das demais obrigações decorrentes deste CONTRATO e do Termo de Referência, calculada sobre o seu valor total, limitada a 10% (dez por cento).

**12.3.4.8.** Compensatória de 20% (vinte por cento) do valor da contratação, caso a **CONTRATADA** dê causa à extinção do CONTRATO, sem motivo justificado e aceito pelo **CONTRATANTE**.

**12.4.** As penalidades serão aplicadas, salvo se houver motivo de força maior ou caso fortuito, justificado e aceito, a critério exclusivo do **CONTRATANTE**.

**12.5.** A soma das penalidades não excederá a 30% (trinta por cento) do valor total do CONTRATO.

**12.6.** As penalidades são independentes, ou seja, a aplicação de uma não exclui a das outras, devendo ser recolhidas ou descontadas de pagamentos eventualmente devidos pelo **CONTRATANTE**, em até 5 (cinco) dias úteis contados a partir de sua comunicação à **CONTRATADA** ou, ainda, se for o caso, cobradas judicialmente.

**12.7.** O não recolhimento das multas no prazo previsto ensejará a incidência de atualização monetária e juros moratórios, calculados em conformidade com a Lei Municipal nº 13.275/2002 e sujeitará a **CONTRATADA** à aplicação do disposto no artigo 156, §8º da Lei Federal nº 14.133/2021.

**12.8.** A aplicação das sanções previstas neste CONTRATO não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao **CONTRATANTE**.

**12.9.** A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à **CONTRATADA**, observando-se o procedimento previsto no *caput* e parágrafos do artigo 158 da Lei Federal nº 14.133/2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

**12.10.** As penalidades serão obrigatoriamente registradas no SICAF.

**12.11.** As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do artigo 163 da Lei Federal nº 14.133/2021.

**12.12.** No caso de aplicação de eventuais penalidades, será observado o procedimento previsto no Título IV, do Capítulo I, da Lei Federal nº 14.133/2021.

### **CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL**

**13.1.** O CONTRATO será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes.

**13.2.** O CONTRATO poderá ser extinto antes do prazo nele fixado, independentemente de interpelação judicial ou extrajudicial, nas hipóteses previstas na Lei Federal nº 14.133/2021.

**13.3.** De acordo com o artigo 106, inciso III, da Lei Federal nº 14.133/2021, o **CONTRATANTE** poderá extinguir o presente CONTRATO, sem ônus, quando não dispuser de créditos orçamentários para a sua continuidade ou quando o CONTRATO não mais lhe oferecer vantagem, observadas as condições previstas no §1º desse dispositivo legal.

**13.4.** A alteração social ou a modificação da finalidade ou da estrutura da **CONTRATADA** não ensejará a extinção se não restringir sua capacidade de concluir o CONTRATO.

**13.5.** Se a operação implicar mudança da pessoa jurídica **CONTRATADA**, deverá ser formalizado termo aditivo para alteração subjetiva.

**13.6.** O termo de extinção, sempre que possível, será precedido:

**13.6.1.** Do balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

**13.6.2.** Da relação dos pagamentos já efetuados e ainda devidos;

**13.6.3.** Das indenizações e multas.

**13.7.** O CONTRATO poderá ser extinto caso se constate que a **CONTRATADA** mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade **CONTRATANTE** ou com agente público que tenha desempenhado função na contratação direta, 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.

#### **CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES**

**14.1.** Eventuais alterações contratuais reger-se-ão pela disciplina dos artigos 124 e seguintes da Lei Federal nº 14.133/2021.

**14.2.** As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da assessoria jurídica do **CONTRATANTE**.

**14.3.** Registros que não caracterizam alteração do CONTRATO podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do artigo 136 da Lei Federal nº 14.133/2021.

#### **CLÁUSULA DÉCIMA QUINTA – DOTAÇÃO ORÇAMENTÁRIA**

**15.1.** As despesas resultantes do presente instrumento correrão por conta dos recursos constantes da(s) dotação(ões) orçamentária(s) \_\_\_\_\_ - \_\_\_\_\_ e, no próximo exercício, se for o caso, à conta da(s) dotação(ões) orçamentária(s) prevista(s) para atender a despesas da mesma natureza.

#### **CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS**

**16.1.** Aplicam-se ao presente a Lei Federal nº 14.133/2021, o Decreto Municipal nº 62.100/2022 e legislação correlata, e, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado, inclusive as específicas para o objeto contratado.

### **CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO**

**17.1.** Incumbirá ao **CONTRATANTE** divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no artigo 94 da Lei Federal nº 14.133/2021, bem como no respectivo sítio oficial na Internet, em atenção ao artigo 91, caput, da Lei Federal nº 14.133/2021.

### **CLÁUSULA DÉCIMA OITAVA– FORO**

**18.1.** Fica eleito o Foro da Comarca desta Capital para solução de quaisquer litígios relativos ao presente CONTRATO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

### **CLÁUSULA DÉCIMA NONA – DA ANTICORRUPÇÃO**

**19.1.** Para a execução deste CONTRATO, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta, quanto ao objeto deste CONTRATO, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma, conforme disposto no artigo 114, inciso II, do Decreto Municipal nº 62.100/2022.

### **CLÁUSULA VIGÉSIMA – ASSINATURA**

**20.1.** O presente instrumento será firmado pelas partes, preferencialmente na forma digital, por meio de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, observados os padrões definidos pela referida infraestrutura.

**20.1.1.** O procedimento para assinatura digital, bem como de verificação de autenticidade, e data de emissão do CONTRATO, se dará em conformidade com o estabelecido na Portaria SG/GAB nº 03/2021, observando-se a Medida Provisória nº 2.200-2 de 24/08/2001, Leis Federais nºs 11.419/2006 e 12.682/2012.

**20.2.** Eventuais instrumentos decorrentes do presente CONTRATO também serão firmados pelas partes preferencialmente na forma digital.

E, por estarem de acordo, as partes firmam o presente, para um só efeito, sem rasuras ou emendas, depois de lido e achado conforme.

Caso firmado fisicamente, as partes o assinam em duas vias de igual teor.

São Paulo, <preencher a data se for documento físico>



**TRIBUNAL DE CONTAS DO MUNICÍPIO DE  
SÃO PAULO**

**DOMINGOS DISSEI**

Presidente

**<DENOMINAÇÃO SOCIAL DA EMPRESA>**

**<NOME DO REPRESENTANTE>**

<Cargo do representante>