# PREGÃO ELETRÔNICO nº 034/2024
# Proc. Adm. nº 240319028916000/2024

## CONTRATANTE
MUNICÍPIO DE SANTANA DE PARNAÍBA - SP
**(EDITAL OBJETIVANDO CONTRATO ADMINISTRATIVO)**

## OBJETO
**Contratação de empresa especializada para fornecer SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES COMPLEMENTARES DE SEGURANÇA DE REDES E APLICAÇÕES, por um período de 48 (quarenta e oito) meses**.

## VALOR TOTAL ESTIMADO DA CONTRATAÇÃO
**R$ 11.829.883,80 (onze milhões, oitocentos e vinte e nove mil, oitocentos e oitenta e três reais e oitenta centavos).**

## DATAS E HORÁRIOS (de Brasília)
DE RECEBIMENTO DAS PROPOSTAS:
**Das 17h15min do dia 29/07/2024 às 09h30min do dia 12/08/2024.**
DA ABERTURA DAS PROPOSTAS:
**A partir das 09h31min do dia 12/08/2024.**
DO INÍCIO DA SESSÃO PÚBLICA DE DISPUTA DE PREÇOS:
**A partir das 10h00min do dia 12/08/2024.**
**LOCAL:**
**www.portaldecompraspublicas.com.br**
"Acesso identificado mediante cadastro"

## CRITÉRIO DE JULGAMENTO
MENOR PREÇO GLOBAL (COM DISPUTA GLOBAL).

## MODO DE DISPUTA
ABERTO.

## PREFERÊNCIA ME/EPP/EQUIPARADAS
SIM.

## RESERVA DE COTAS ME/EPP/EQUIPARADAS
NÃO.

## INVERSÃO DAS FASES DE HABILITAÇÃO E JULGAMENTO
NÃO.

## E-MAIL PARA CONTATO REFERENTE A ESTE EDITAL
alessandro.33242@santanadeparnaiba.sp.gov.br e/ou smcl@santanadeparnaiba.sp.gov.br

# Sumário

**PREGÃO ELETRÔNICO Nº XXX/2024**
**Proc. Adm. nº 240319028916000/2024**

**O MUNICÍPIO DE SANTANA DE PARNAÍBA** torna público para o conhecimento dos interessados, que realizará licitação na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto Municipal nº 4.990, de 28 de dezembro de 2023, da Lei Complementar 123/2006, bem como as normas contidas nesse Edital e seus anexos e demais legislações aplicáveis.

## 1. DO OBJETO

1.1. **O objeto da presente licitação é a Contratação de empresa especializada para fornecer SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES COMPLEMENTARES DE SEGURANÇA DE REDES E APLICAÇÕES, por um período de 48 (quarenta e oito) meses.**

1.2. A licitação será regida conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos, dividida em itens/lotes, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos itens/lotes for de seu interesse.

## 2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. A participação neste Pregão está condicionada ao **cadastramento e aprovação da inscrição do licitante** junto ao sistema eletrônico de licitações adotado: **Portal de Compras Públicas – "WCOMPRAS"** (conforme termos definidos no site da empresa em https://www.portaldecompraspublicas.com.br/adesao/fornecedor), em tempo hábil para ocorrer o cadastramento das propostas no sistema.

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento realizado por meio de sistema eletrônico fornecido por pessoa jurídica de direito privado, devendo o custo de operacionalização e uso do sistema ficar a cargo do licitante, nos termos definidos na referida plataforma.

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

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. Neste certame não serão reservadas cotas de até 25% do presente objeto ou itens exclusivos para ME/EPP/EQUIPARADAS, considerando o que preceitua o Art. 49, incisos II e III da LC 123/06, nas justificativas do Termo de Referência e das Complementares do Anexo II.

2.5. Será concedido tratamento favorecido para as participantes ME/EPP/EQUIPARADAS, no que se refere ao empate ficto e à possibilidade de comprovação da regularidade fiscal e trabalhista postergadas, nos limites previstos nos Arts. 42 a 45 da Lei Complementar nº 123, de 14 de dezembro de 2006, e conforme disciplinado pelo Art. 4º da Lei Federal 14.133/2021.

2.6. Não poderão disputar esta licitação:

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

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

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

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

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

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

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

2.6.8. Agente público do órgão ou entidade licitante;

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

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

2.6.11. Das pessoas jurídicas em processo de falência;

2.6.12. De empresas consorciadas em mais de um consórcio ou participando de um consórcio e também isoladamente, conforme inciso IV do art. 15 da Lei nº 14.133, de 2021;

2.6.13. De tipos societários não permitidos para atuar no ramo/objeto do certame.

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

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

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

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

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

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

## 3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

3.2. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e nos prazos estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.11.1 deste Edital.

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

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

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

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

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

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

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

3.5.1. Em caso de itens exclusivos para participação de microempresas e empresas de pequeno porte, somente com a assinalação do campo será possível o prosseguimento no cadastramento de proposta no certame (considerando a total responsabilidade da participante nesta declaração, ciente da possibilidade de aplicação de sanções em caso de declaração falsa);

3.5.2. Para itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a não assinalação do referido campo produzirá o efeito de o licitante não

ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.6. A falsidade da declaração de que trata os itens 3.3 ou 3.5 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.7. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a data e horário definido para Abertura de Proposta, conforme consta no preambulo deste edital.

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

3.9. Os documentos que compõem a proposta dos licitantes que foram convocados, serão disponibilizados aos participantes após a fase de lances.

3.9.1. **O acesso à documentação disponível se dará através de solicitação por e-mail ao Pregoeiro(a), que será atendida assim que possível**.

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

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

3.10.2. Se disponibilizado, os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima, observadas as instruções da Normativa SEGES nº 73/2022 ao que se aplicar.

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

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

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

3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.10 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

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

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

## 4. DO PREENCHIMENTO DA PROPOSTA

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

4.1.1. Valores unitários e totais do item (ou desconto, conforme cada caso);

4.1.2. Marca e/ou Fabricante;

4.1.3. Descritivo do item ofertado (conforme edital);

4.1.4. Validade da Proposta (mínimo de 60 dias).

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

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

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

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

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

4.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão, se aplicável ao objeto, se beneficiar do regime de tributação pelo Simples Nacional.

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

4.8.1. O prazo de validade da proposta não será inferior a **60 (sessenta)** dias**,** a contar da data de sua apresentação.

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

4.8.3. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos.

4.9. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas Estado de São Paulo e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do 32 e 33 da Constituição Estadual, bem como art. 1º da Lei Complementar Estadual nº 709, de 1993; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

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

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

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

5.3. O sistema disponibilizará campo próprio para troca de mensagens que ficará ativo somente durante a negociação de valores entre o Pregoeiro e o licitante melhor colocado.

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

5.5. O lance deverá ser ofertado pelo **valor global**.

5.5.1 Em se tratando de Lotes ou de Valor Global, serão observados eventuais casos de sobrepreço em itens específicos, ou ainda descontos em somente um dos itens, sendo correto o **desconto linear** e mais equalizado possível com a proposta inicial da empresa, e ainda em observância também à estimativa de preços desse município.

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

5.7. O licitante somente poderá oferecer *lance de valor inferior ou percentual de desconto superior* ao último por ele ofertado e registrado pelo sistema (podendo ofertar lances "intermediários" maiores que o lance vencedor com o objetivo de ficar melhor colocado ao término da disputa).

5.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 0,01 (um centavo).

5.9. O licitante poderá solicitar a exclusão de seu último lance ofertado, que será analisado pelo pregoeiro, nas hipóteses de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa adotado e indicado no preâmbulo do edital, observando as regras abaixo dispostas a depender de cada opção:

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

5.10.1.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

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

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

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

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

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

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

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

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

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

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

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

5.10.3.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 5.10.3, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

5.10.3.2. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

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

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

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

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

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

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

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

5.14. 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.

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

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

5.17. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática do melhor valor e dos subsequentes. Caso a primeira colocada seja uma empresa de maior porte, aplica-se o disposto nos Arts. 44 e 45 da Lei Complementar nº 123, de 2006, exceto nos casos previstos no Art. 4º da Lei Federal 14.133/2021, que dispensa o tratamento diferenciado e favorecido para microempresas e empresas de pequeno porte em determinadas situações.

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

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

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

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

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

5.18.1. 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:

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

5.18.1.2. 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;

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

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

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

5.18.2.1. 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;

5.18.2.2. Empresas brasileiras;

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

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

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

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

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

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

5.19.4. O resultado da negociação será divulgado a todos os licitantes (no chat do certame e na Ata de Sessão) e anexado aos autos do processo licitatório.

5.19.5. O pregoeiro solicitará ao licitante melhor classificado que, no prazo de **24 (vinte e quatro) horas**, envie a proposta readequada condizente com o último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.19.6. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada e encaminhada pelo licitante antes de findo o prazo.

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

## 6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta?cadastro=1&ordenarPor=nomeSancionado&direcao=asc); e

6.1.2. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União(https://portaldatransparencia.gov.br/sancoes/consulta?cadastro=2&ordenarPor=nomeSancionado&direcao=asc);

6.1.3. Relação de Apenados disponível no site do Tribunal de Contas do Estado de São Paulo - TCE-SP (https://www.tce.sp.gov.br/pesquisa-relacao-apenados);

6.1.4. Consulta Consolidada de Pessoa Jurídica no Portal do TCU (https://certidoes-apf.apps.tcu.gov.br/);

6.1.5. Consulta ao sistema de Certidões da Controladoria-Geral da União - CGU, mais especificamente a referente à Certidão negativa correcional (ePAD, CGU-PJ, CEIS, CNEP e CEPIM) – (https://certidoes.cgu.gov.br/);

6.1.6. SICAF – Sistema de Cadastro Unificado de Fornecedores (https://www3.comprasnet.gov.br/sicaf-web/public/pages/consultas/consultarRestricaoContratarAdministracaoPublica.jsf).

6.2. As consultas específicas junto ao CEIS e ao CNEP tratadas nos itens 6.1.1 e 6.1.2 não são obrigatórias quando as informações já constarem nas consultas do TCU e da CGU.

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

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

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

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

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

6.5. Na hipótese de inversão das fases de habilitação e julgamento, caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.6. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o item 3.5 e demais regras desse edital e da legislação aplicável.

6.7. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

6.8. Será **desclassificada** a proposta vencedora que:

6.8.1. Contiver vícios insanáveis;

6.8.2. Não obedecer às especificações técnicas contidas no Termo de Referência;

6.8.3. Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação após a disputa e/ou negociação;

6.8.4. Não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.8.5. Apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

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

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

6.9.1.1. Que o custo do licitante ultrapassa o valor da proposta; e

6.9.1.2. Inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

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

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

6.10.2. No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado e pela superação de custo unitário em itens relevantes;

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

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

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

6.12. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

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

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

6.12.3. Caso a produtividade for diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo

ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

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

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

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

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

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

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

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

6.16. Quando houver apresentação de amostra, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, por meio de mensagem no chat do sistema, cuja presença será facultada a todos os interessados, incluindo os demais licitantes (devendo apresentar documento de identificação pessoal e procuração ou outro documento idôneo para comprovar os poderes e o interesse do licitante).

6.17. Os resultados das avaliações serão divulgados por meio de mensagem e/ou juntada de documento no sistema.

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

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

## 7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos no Anexo IV, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação através de convocação no chat da sessão (para envio conforme item 5.19.5), nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021, juntamente com a proposta comercial readequada.

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

resguardadas eventuais diferenças de exigências que deverão ser complementadas observando sempre as regras dispostas neste edital.

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

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

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

7.3.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 20% (vinte por cento) para o consórcio em relação ao valor exigido para os licitantes individuais.

7.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, emitidos pela internet ou por cópia autenticada ou simples (sempre passível de diligência em caso de dúvidas).

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

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

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

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

7.8. Para o presente certame a visita técnica é opcional.

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

7.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

7.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

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

7.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf, quando utilizado, serão enviados por e-mail, em formato digital, no prazo de **24 (vinte e quatro) horas**, prorrogável por igual período se solicitado, contado da solicitação do pregoeiro no chat da sessão.

7.11.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da *Instrução Normativa SEGES nº 73, de 30 de setembro de 2022*.

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

7.12.1. Os documentos relativos à regularidade fiscal que constem do Anexo IV somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante melhor classificado.

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

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

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

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

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

7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.11.1.

7.16. Os documentos do licitante cuja proposta atenda ao edital de licitação e que, após concluídos os procedimentos de que tratam os subitens anteriores, reste previamente habilitado, ficarão disponíveis para os participantes;

7.16.1. O acesso à documentação disponível se dará através de solicitação por e-mail ao Pregoeiro(a), que será atendida assim que possível;

7.16.2. Os documentos dos licitantes que tiveram suas propostas recusadas ou que restaram inabilitados, também poderão ser solicitados através de e-mail ao Pregoeiro(a).

7.17. A comprovação da efetiva regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, devendo, porém, apresentarem toda a documentação exigida mesmo que a aqui citada apresente alguma restrição.

7.17.1. Havendo alguma restrição na comprovação da regularidade fiscal ou trabalhista, será assegurado o prazo de 05 (cinco) dias úteis, depois de declarado vencedor, prorrogáveis por igual período, mediante solicitação e a critério desta Prefeitura, para regularização da documentação, pagamento ou parcelamento do débito, e emissão da certidão negativa ou positiva com efeito de certidão negativa;

7.17.2. Este município reserva-se ao direito de poder verificar junto aos órgãos emissores das respectivas certidões, tanto para a averiguação da veracidade destas, quanto para verificar a regularidade de alguma apresentada com restrição, procedendo a reemissão desta se possível.

7.17.3. A não regularização da documentação fiscal ou trabalhista, no prazo previsto no subitem 7.17.1, implicará na perda do direito à contratação e o pregoeiro examinará as ofertas subsequentes e a qualificação dos licitantes, na ordem de classificação, sucessivamente, até a apuração de uma que atenda ao edital para a assinatura do Contrato, ou fracassar a licitação ou o(s) item(s), conforme a situação se apresentar.

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

## 8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto nos artigos 123 e seguintes do Decreto Municipal n.º 4990, de 2023 e no artigo 165 da Lei nº 14.133, de 2021.

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

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

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

8.3.2. O prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.3. O prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação, sendo disponibilizado o mesmo prazo de 3 (três) dias úteis, decorrido o prazo de recurso, para apresentação das contrarrazões de recurso;

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

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

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

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

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

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

8.9. Os autos do processo, em especial a documentação de habilitação e proposta das empresas, permanecerão com vista franqueada aos interessados para instrumentalização das peças recursais, devendo ser solicitado por e-mail quando não estiverem disponíveis no sistema.

8.10. Desde já, fica consignado, em função da desnecessidade de fundamentar a intenção de recurso, que em caso de registrar intenção e deixar de interpor a peça recursal ou interpor recurso com caráter com objetivo meramente **PROTELATÓRIO**, ficará o licitante que der causa a estes fatos, sujeito às seguintes sanções:

8.10.1. **Advertência;**

8.10.2. **Multa de até 10% (dez por cento)** do valor estimado do(s) item(s) que intencionou o recurso.

8.10.3. A sanção de advertência poderá ser aplicada, cumulativamente ou não, à penalidade de multa.

8.10.4. Para aplicação destas penalidades, será aberto processo administrativo, analisado por comissão específica, resguardado o direito ao contraditório e a ampla defesa.

## 9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

9.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. Recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. Pedir para ser desclassificado quando encerrada a etapa competitiva;

9.1.2.4. Deixar de apresentar amostra, catálogo ou ficha técnica; ou

9.1.2.5. Apresentar proposta ou amostra em desacordo com as especificações do edital;

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

9.1.3.1. Recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação.

9.1.5. Fraudar a licitação.

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

9.1.6.1. Agir em conluio ou em desconformidade com a lei;

9.1.6.2. Induzir deliberadamente a erro no julgamento;

9.1.6.3. Apresentar amostra falsificada ou deteriorada;

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

9.1.8. Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

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

9.2.1. Advertência;

9.2.2. Multa;

9.2.3. Impedimento de licitar e contratar; e

9.2.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. A natureza e a gravidade da infração cometida;

9.3.2. As peculiaridades do caso concreto;

9.3.3. As circunstâncias agravantes ou atenuantes;

9.3.4. Os danos que dela provierem para a Administração Pública;

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

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado (ou dos itens participantes), recolhida no prazo máximo de **30 (trinta) dias**, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 15% a 30% do valor do contrato licitado.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do Município de Santana de Parnaíba, pelo prazo máximo de 3 (três) anos.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

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

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

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

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados ao Município de Santana de Parnaíba.

## 10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

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

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, no local de realização do certame (www.portaldecompraspublicas.com.br) nos campos específicos deste certame na plataforma.

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

10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação, observadas as regras trazidas pelo § 2º do artigo 16 da IN SEGES nº 73, de 2022.

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

## 11. DA CONTRATAÇÃO

11.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de **10 (dez) dias úteis**, contados a partir da data de sua convocação pelo Departamento de Contratos

da Secretaria Municipal de Compras e Licitações, para assinar o Contrao, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

11.2. O prazo para assinatura poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

a) solicitação seja devidamente justificada e apresentada dentro do prazo; e

b) a justificativa apresentada seja aceita pela Administração.

11.3. O signatário da empresa convocada deverá informar os dados necessários para preenchimento do Contrato, assim como do Termo de Ciência e Notificação, sendo necessário apresentar cédula de identificação (RG, CNH, etc.) e Procuração, caso não tenha sido apresentada anteriormente ou não seja sócio/administrador da empresa.

11.3.1. A cédula de identificação pode ser dispensada, no caso de utilização de Assinatura Eletrônica (sistema ICP-Brasil, GovBr, etc).

11.3.2. A não apresentação dos documentos solicitados no item 13.3 impedirá a assinatura do Contrato, implicando na aplicação das sanções previstas neste Edital.

11.4. Se por ocasião da formalização do Contrato as certidões de regularidade Fiscal e Trabalhista apresentadas para fins de Habilitação no certame estiverem com os prazos de validade vencidos, este Município poderá verificar a situação por meio eletrônico hábil, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por tais meios;

11.4.1. Se não for possível obtê-las ou atualizá-las por meio eletrônico hábil, o adjudicatário será notificado para que no prazo máximo de 05 (cinco) dias úteis (prazo para atendimento de sua convocação), comprove a situação de regularidade de que trata o item 13.4, mediante a reapresentação das certidões com prazos de validade em vigor, sob pena da contratação não se realizar.

11.4.1.1. No caso de empresas beneficiadas pela LC 123/06 o prazo de que trata o item acima poderá ser prorrogado por até 05 (cinco) dias úteis.

11.5. O preço contratado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência do Contrato.

11.6. Na hipótese de o convocado, dentro do prazo de validade de sua proposta, não assinar o Contrato ou não atualizar as certidões no prazo e nas condições estabelecidas, será instaurado procedimento para apuração e aplicação das sanções cabíveis ao convocado, podendo ser deliberado pelo chamamento de licitante remanescente para assumir a contratação denegada, desde que respeitada a ordem de classificação (com possibilidade de negociação), para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

11.7. O CONTRATADO se obriga a manter, durante toda a vigência do Contrato em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

## 12. DAS DISPOSIÇÕES GERAIS

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

12.2. 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.

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

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

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

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

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

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

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

12.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e nos sites do Portal de Compras Públicas e desta Administração Municipal.

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

12.11.1. ANEXO I – Termo de Referência

12.11.2. ANEXO I.a. – Especificações Detalhadas

12.11.3. ANEXO I.b. – Requisitos de Atendimento do SOC

12.11.4. ANEXO I.c. – Termo de Confidencialidade e Proteção de Dados

12.11.5. ANEXO II – Justificativas Complementares

12.11.6. ANEXO III – Planilha de Itens e Valores Estimados

12.11.7. ANEXO IV – Relação de Documentos de Habilitação

12.11.8. ANEXO V – Modelo de Proposta Comercial Escrita

12.11.9. ANEXO VI – Minuta de Termo de Contrato

Santana de Parnaíba, 25 de julho de 2024.

***CLEUSA CARVALHO***
***AUTORIDADE COMPETENTE***

# ANEXO I

## *Termo de Referência*

**SECRETARIA GESTORA: SECRETARIA MUNICIPAL DE TECNOLOGIA DA INFORMAÇÃO**

### 1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa especializada para fornecer SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES COMPLEMENTARES DE SEGURANÇA DE REDES E APLICAÇÕES, por um período de 48 (quarenta e oito) meses, conforme requisição 1846/2024 - SMTI.

| ITEM | DESCRIÇÃO | QUANTIDADE |
|---|---|---|
| 1 | SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES | 48 |
| 2 | SERVIÇO DE RESPOSTA A INCIDENTES CIBERNÉTICOS | 48 |
| 3 | SERVIÇOS TÉCNICOS CONTINUADOS DE SOLUÇÕES CISCO | 15 |
| 4 | SERVIÇOS TÉCNICOS DE WIFI | 15 |
| 5 | SERVIÇO DE TREINAMENTO DAS SOLUÇÕES (NGFW, VPN, MFA, NAC, DNS, MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E EXPERIÊNCIA DIGITAL) | 1 |
| 6 | SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DAS SOLUÇÕES NGFW, VPN, MFA, NAC, DNS, MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E EXPERIÊNCIA DIGITAL | 48 |
| 7 | HORAS DE CONSULTORIA PARA SOLUÇÃO DE MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES | 400 |

1.2. **Da natureza do objeto**

1.2.1. O(s) bem(ns) e serviço(s) objeto desta contratação são caracterizados como **comuns**, uma vez que se trata de equipamentos para infraestrutura de redes que estão presentes em grandes empresas e em grande número e os padrões de desempenho e qualidade podem ser objetivamente definidos, por meio de especificações usuais no mercado.

1.2.2. O objeto desta contratação enquadra-se na modalidade de **SERVIÇO(S)** comuns para fins do disposto no art. 118 do Decreto Municipal nº 4.990/2023 e incisos XIII e XLI do art. 6º da Lei Federal 14.133/2021, tendo em vista que seu padrão de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado.

1.2.3. O Município não possui catálogo eletrônico de padronização de compras, serviços e obras. Embora a legislação permita a utilização/adoção do catálogo do Poder Executivo Federal por todos os entes federativos, atualmente este catálogo é composto apenas por alguns itens. Sendo assim, a não utilização deve-se ao fato dos referidos órgãos não possuírem catálogos padronizados para o objeto em questão..

1.3. **Do prazo da contratação**

1.3.1. O prazo de vigência da contratação é de 48 (quarenta e oito) meses contados da emissão da ORDEM DE SERVIÇO, prorrogáveis para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.3.2. Por se tratar de um serviço contínuo, o “Item 6 - SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

DAS SOLUÇÕES NGFW, VPN, MFA, NAC, DNS, MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E EXPERIÊNCIA DIGITAL" será parcelado em 48 (quarenta e oito) meses.

1.3.3. Os hardwares que fazem parte do "Item 1 - SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES" deverão ser entregues em regime de comodato durante a vigência do contrato e prorrogações na forma da lei.

1.4. **Do não parcelamento do objeto:**

O objeto será agrupado em **lote único** pelo fato de que o fornecedor deverá efetuar configurações e integrações entre todos os produtos. O agrupamento de itens também permite o alcance de maior eficiência não só no âmbito da funcionalidade da contratação, como também naquele relacionado à prevenção de contratações conflituosas e, por conseguinte, redução de conflitos entre fornecedores distintos. O modelo de contratação pretendido permite a preservação do funcionamento integrado, não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, o suporte técnico e o treinamento serão executados por um único fornecedor por grupo. Dessa forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução.

1.5. A contratação do objeto pretendido tem amparo na Lei Nº 14.133/2021, no que couber, e demais legislações aplicadas à matéria.

1.6. **Alinhamento entre a contratação e o planejamento**

1.6.1. Considerando que no inciso VII do caput do artigo 12º da Lei 14.133/2021, a elaboração do Plano de Contratação Anual necessita de regulamentação pelo ente federativo, e o Ato que regulamentou no âmbito do Município de Santana de Parnaíba foi o Decreto Municipal nº 5.023/2024 que entrou em vigor em 29 de fevereiro de 2024, sendo assim, não foi elaborado o PCA para o exercício de 2024, porém todas as contratações estão alinhadas com a Lei Orçamentária Anual do respectivo exercício.

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

2.1. A solução consiste em um Firewall de Próxima geração com recursos avançados de segurança, solução de DNS recursivo para aumentar a proteção dos usuários, assim como proteger o acesso dos alunos em redes onde não passem pelo firewall principal, possibilitando regras de bloqueio e monitoramento dos acessos, contemplando o hardware, licenciamento, implantação, configuração, treinamento e atualizações, incluindo, garantia por 48 (quarenta e oito) meses, conforme descrição detalhada dos itens no ANEXO I.a deste Termo de Referência.

2.2. O produto deve fornecer proteção robusta e avançada contra ameaças cibernéticas em redes corporativas e ambientes de negócios.

2.3. Deve fornecer atualizações regulares de firmware e patches de segurança para garantir que o Firewall esteja atualizado e protegido contra as últimas ameaças cibernéticas.

2.4. Avaliar os serviços já existentes na rede da Prefeitura das soluções Cisco, com monitoramento e performance das aplicações desenvolvidas pela Prefeitura e experiência digital dos usuários da rede.

2.5. Para efeitos de atualização de firmware e patches de segurança, bem como suporte técnico, o fornecedor deverá atender à Prefeitura, sem custo adicional, por período **não inferior a 48 (quarenta e oito)**

**meses**.

2.6. A solução deverá ser constituída dos equipamentos relacionados nos itens, sendo preferencialmente de um mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles.

2.7. A escolha do agrupamento dos itens em grupo visa a plena qualificação da empresa fornecedora que prestará os serviços de instalação e configuração, bem como prestará os serviços de suporte durante a vigência do contrato de garantia dos equipamentos, a total compatibilidade entre os equipamentos solicitados, a redução de custos operacionais e de infraestrutura física, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total de propriedade

## 3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A presente contratação justifica-se atender as necessidades de segurança dos sistemas de informação da Prefeitura, bem como proporcionar o acesso seguro aos Serviço de Rede hospedados nos servidores.

3.2. Uma solução de Firewall é responsável por atender às seguintes necessidades:

3.2.1. Proteção contra ameaças externas: O firewall é a primeira linha de defesa contra ataques cibernéticos, como vírus, malware e ransomware. Ele analisa o tráfego de entrada e saída da rede, bloqueando os pacotes de dados que apresentam sinais de ameaça.

3.2.2. Controle de acesso: Permite que sejam definidas regras de acesso à rede, garantindo que apenas usuários autorizados tenham permissão para acessar os recursos internos.

3.2.3. Separação de redes: Implementa separação de redes, ajudando a proteger os dados confidenciais da Instituição de acessos não autorizados.

3.2.4. Auditoria de segurança: O firewall mantém registros de todos os eventos de segurança que ocorrem na rede. Esses registros podem ser usados para investigar incidentes de segurança e para melhorar a segurança da rede.

3.2.5. Atualmente a Prefeitura conta com a Solução de Firewall de Próxima Geração Cisco ASA, proporcionando proteção aos seus respectivos equipamentos conectados à Rede. Para que essa proteção seja efetiva, é necessário que cada Firewall possua uma assinatura vigente de features, além de suporte e garantia, que prevê a distribuição de atualizações de software e definições de ameaças, bem como a manutenção dos componentes de hardware em caso de falha e soluções de problemas mais específicos no uso do equipamento.

3.2.6. Verificou-se junto ao fabricante que o atual Appliance de Firewall (equipamento) da Prefeitura (adquirido ainda em 2014) está em processo de descontinuação (End of Life) desde 2021, além de que a capacidade da solução atual não atende as demandas da Prefeitura, o que provocará perda no principal ativo de segurança da informação que temos hoje operando na Prefeitura. Diante do cenário, será necessário fazer a aquisição de outro appliance permitindo a continuidade das atuais configurações de segurança de rede.

3.2.7. Caso não seja feita a aquisição de um novo equipamento, o atual firewall deixará de receber novas definições para a detecção de ameaças, filtros de conteúdo (url, aplicações, redes, etc), a utilização da VPN

também ficará sem a aplicação Global Protect, sendo necessária uma reconfiguração em todos os acessos VPN nos clientes, elevará drasticamente o risco de incidentes de Segurança na Rede institucional. Além de não ser possível utilizar toda a banda de internet disponível, uma vez que o link que dispomos é superior à capacidade do Firewall atual.

3.2.8. O objeto da contratação também está alinhado com o Plano Diretor de Tecnologia da Informação (PDTI), conforme demonstrado abaixo.

| ALINHAMENTO AO PDTI | | | |
|---|---|---|---|
| ID | Descrição | ID | Meta |
| A-037 | Implantar um Processo de Resposta a Incidentes de Segurança da Informação | M-037 | 1 Processo de resposta a incidentes implantado e revisado anualmente |
| A-041 | Revisar a arquitetura de segurança da informação e adquirir os serviços, soluções e equipamentos que forem necessários para atender às necessidades de disponibilização de dados, auditoria, defesa em camadas e segmentação de ambientes | M-041 | 1 Arquitetura revisada e plano de ação documentado<br>2 Firewalls de borda implantados |
| A-090 | Plano de aquisição e implementação de ferramenta para análise de performance e automação de rede e segurança e correção automática de problemas | M-090 | Integração com toda a parte de infraestrutura e servidores |

## 4. REQUISITOS DA CONTRATAÇÃO

4.1. REQUISITO 1: Atualizar o componente de hardware da solução de Firewall da Prefeitura, com o menor impacto possível nas configurações de software (possibilidade de migração das regras e demais configurações implementadas atualmente).

4.2. REQUISITO 2: Viabilizar a atualização contínua dos elementos de software da Solução de Firewall da Prefeitura.

4.3. REQUISITO 3: Manter a alta disponibilidade da solução de Firewall, por meio da implementação de esquema de redundância.

4.4. REQUISITO 4: Viabilizar e implementar políticas de segurança e autenticação à rede.

4.5. REQUISITO 5: Implementar monitoração da performance das aplicações e experiência digital dos usuários de modo a garantir que os sistemas fiquem o maior tempo possível online, sem interrupções.

4.6. REQUISITO 6: Ajustar as configurações da infraestrutura atual, de modo a aumentar a confiabilidade da rede e diminuir as interrupções dos serviços de rede cabeada e wifi.

4.7. REQUISITO 9: Avaliação da infraestrutura de rede Cisco, de acordo as boas práticas do fabricante

**Requisitos de Capacitação**

4.8. Será necessário treinamento para parte da equipe que atuará com a solução. O treinamento deverá ter a duração mínima conforme cada solução descrito abaixo:

| Solução | Repasse de conhecimento (não oficial) - Carga horária mínima | Treinamento não oficial para _ pessoas | Treinamento oficial - Carga horária mínima | Treinamento oficial para _ pessoas |
|---|---|---|---|---|
| SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO COM IPS, CONTROLE DE APLICAÇÕES, VPN E AUTENTICAÇÃO MULTIFATOR | 40 horas | 04 | 40 horas | 03 |
| SOLUÇÃO DE POLÍTICA DE SEGURANÇA E AUTENTICAÇÃO À REDE (NAC) | 40 horas | 04 | 40 horas | 03 |
| SOLUÇÃO DE PROTEÇÃO DE DNS RECURSIVO | - | - | 24 horas | 04 |
| SOLUÇÃO DE MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E MONITORAMENTO DE EXPERIÊNCIA DIGITAL | 24 horas | 04 | 40 horas | 08 |

4.9. A soma da carga horária do treinamento das soluções de Monitoramento de Performance de Aplicações e Monitoramento da Experiência Digital, somados deve ser de no mínimo 24 horas para o não oficial e 40 horas para o oficial, caso o fabricante da solução possua um único treinamento que aborde as duas soluções, este deverá ter a carga horária mínima de 40 horas.

**Requisitos Legais**

4.10. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, o Decreto Municipal 4.990/2023, subsidiariamente das disposições contidas na Instrução Normativa SGD/ME nº 94, de 2022 no que se aplicarem em âmbito municipal, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e a outras legislações aplicáveis;

**Requisitos de Manutenção**

4.11. Devido às características da solução, há necessidade de realização de atualizações e suporte técnico pela Contratada, visando à manutenção da disponibilidade da solução por um período de 48 (quarenta e oito) meses.

4.12. A modalidade de suporte a ser disponibilizado deverá ser 24x7, com substituição avançada de peças (24 horas por dia, 07 dias por semana), durante o horário normal de trabalho, sendo que todos os serviços on site deverão ser de responsabilidade da CONTRATADA.

**Requisitos Temporais**

4.13. A Entrega dos equipamentos físicos deverá ser efetivada no prazo máximo de 60 (sessenta) dias corridos, a contar da emissão da ORDEM DE FORNECIMENTO pela CONTRATANTE por parte da Secretaria Municipal de Tecnologia da Informação (SMTI) e recebimento da CONTRATADA, podendo ser prorrogada, excepcionalmente, desde que justificado previamente pela Contratada e autorizado pelo Contratante;

4.14. Os prazos poderão eventualmente ser prorrogados, se houver justificativa plausível e fundamentada, desde que solicitada com antecedência e seja aceita pela Secretaria requisitante;

4.15. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.16. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

4.17. O Serviço de manutenção e suporte técnico deverá abranger a manutenção corretiva com cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a substituição de peças, partes, componentes e acessórios.

4.18. A modalidade de suporte a ser disponibilizado deverá ser 24x7 (24 horas por dia, 07 dias por semana) de responsabilidade da CONTRATADA.

4.19. **Todas as peças e componentes mecânicos ou eletrônicos substitutos deverão ser originais ou certificados pelo fabricante e sempre "novos e de primeiro uso", não podendo ser recondicionados.**

**Requisitos de Segurança e Privacidade**

4.20. A Contratada deverá guardar sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

4.21. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se no ANEXO I.c. - TERMO DE CONFIDENCIALIDADE E PROTEÇÃO DE DADOS

**Requisitos Sociais, Ambientais e Culturais**

4.22. Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

4.23. A abertura de chamados técnicos e encaminhamentos de demandas deverão ser realizados, preferencialmente, sob a forma eletrônica, evitando-se a impressão de papel. Além disso, as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia.

**Requisitos da Arquitetura Tecnológica**

4.24. Os bens adquiridos deverão ser instalados e os serviços executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica do CONTRATANTE.

4.25. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pelo CONTRATANTE. Caso não seja autorizada, é vedado à CONTRATADA adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pelo CONTRATANTE.

**Requisitos de Garantia e Manutenção**

4.26. Todos os PRODUTOS fornecidos deverão possuir garantia de funcionamento, serviços de manutenção e suporte técnico, por um período de 48 (quarenta e oito) meses, a contar da data de emissão do termo de aceite dos produtos.

4.27. O serviço de manutenção deverá ser prestado nas dependências da PREFEITURA, exceto para as soluções de VPN, MFA, NAC, DNS Recursivo, Monitoramento e Performance de Aplicações e Monitoramento de Experiência Digital.

4.28. O Serviço de manutenção e suporte técnico dos produtos deverão abranger a manutenção corretiva com cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a substituição de peças, partes, componentes e acessórios.

4.29. Para equipamentos físicos, a modalidade de suporte a ser disponibilizado deverá ser 24x7x4, com substituição avançada de peças, sendo entregues dentro de quatro horas de determinação de que a peça a ser substituída é realmente necessária (24 horas por dia, 07 dias por semana), durante o horário normal de trabalho, sendo que todos os serviços on site deverão ser de responsabilidade da CONTRATADA.

4.30. Com o objetivo de manter os equipamentos a serem fornecidos em boas condições de funcionamento ou restabelecê-lo a tais condições, a CONTRATADA prestará serviço de assistência técnica on-site durante o período de disponibilidade para as soluções, exceto as soluções de VPN, MFA, NAC, DNS Recursivo, Monitoramento e Performance de Aplicações e Monitoramento de Experiência Digital.

4.31. O prazo para a CONTRATADA iniciar o atendimento via suporte técnico para diagnóstico do problema é de, no máximo, 30 (trinta) minutos, contado a partir da abertura do chamado e dentro do período de disponibilidade.

4.32. Proporcionar assistência técnica on-site comparecendo no prazo de até 04 (quatro) horas no local (tempo de chegada), contado a partir da abertura do chamado e dentro do período de disponibilidade.

4.33. O prazo máximo de reparo e solução, contado a partir do chamado e dentro do período de disponibilidade é de 06 (seis) horas úteis, para os PRODUTOS fornecidos.

4.34. Para as soluções de Subscrição ou SaaS, o tempo de solução deverá ser de no máximo 06 (seis) horas. Caso haja eventual indisponibilidade acima do prazo de 06 (seis) horas, a CONTRATADA deverá apresentar todas as devidas justificativas do Fabricante à PREFEITURA, além de acompanhar a evolução da restauração completa do serviço, para que não ocorra penalidades.

4.35. A CONTRATADA deverá assegurar a assistência técnica necessária à satisfatória utilização dos equipamentos, no que consiste à manutenção de hardware, instalação, reinstalação e atualização de softwares/firmwares internos dos equipamentos.

4.36. Para prestação do serviço de garantia será exigido que a CONTRATADA habilite o suporte junto ao Fabricante, para todos os equipamentos relacionados

4.37. A CONTRATADA deverá disponibilizar para a PREFEITURA, durante o período de vigência da garantia, acesso automático às documentações e as versões de manutenção e atualizações de software/firmwares dos PRODUTOS, via portal web internet do fabricante, sob demanda, sem ônus à PREFEITURA.

4.38. A CONTRATADA deverá ter acesso direto ao suporte técnico especializado do Fabricante dos PRODUTOS, via telefone e e-mail, para solução dos problemas e encaminhamento dos problemas ao setor competente do Fabricante. Deve também disponibilizar uma senha de acesso para este serviço a equipe da PREFEITURA.

4.39. A PREFEITURA poderá solicitar a revisão sobre os resultados entregues na realização dos serviços que tenham sido feitos fora do escopo acordado no Contrato e/ou das normas, padrões, procedimentos e instruções técnicas da PREFEITURA, ou ainda em desacordo com a legislação vigente, ficando a CONTRATADA obrigada a refazer o serviço conforme obrigação estabelecida neste Contrato, sem ônus para a PREFEITURA.

4.40. Todo resultado entregue a partir dos serviços realizados pela CONTRATADA terá garantia de correções e ajustes necessários durante os 90 (noventa) dias seguintes à conclusão daqueles serviços, mesmo que essa conclusão tenha ocorrido nos últimos 90 (noventa) dias do Contrato.

4.41. Dentro do período de garantia, a correção de erros nos serviços entregues pela CONTRATADA deverá ser efetuada sem qualquer ônus para a PREFEITURA, seja financeiro ou de atraso na prestação de outro(s) serviço(s), desde que, comprovadamente, não tenham se dado em razão das especificações feitas pela PREFEITURA.

4.42. A garantia do produto é estabelecida considerando-se a versão de Software entregue e futuras versões de Software.

4.43. A correção deverá ser executada pela CONTRATADA no prazo máximo de 24 (vinte e quatro) horas úteis, contadas a partir do comunicado feito pela PREFEITURA junto à CONTRATADA sobre o defeito encontrado.

4.44. Extinta a vigência do CONTRATO, a CONTRATADA terá 05 (cinco) dias úteis para atendimento.

4.45. Caso a CONTRATADA entenda necessária, em um serviço específico, a dilatação dos prazos definidos, deverá justificar-se tecnicamente por meio de relatório formal.

4.46. Caso a PREFEITURA não aceite as argumentações, não haverá interrupção na contagem do prazo

definido previamente.

4.47. A não observância ao prazo para correção de defeito implica na aplicação das penalidades cabíveis.

4.48. Terminada a correção pertinente, a CONTRATADA enviará para o responsável pelo(s) artefato(s), designado pela PREFEITURA, com cópia para a Gestão do Contrato, o(s) artefato(s) corrigido(s). A data e hora do envio deste comunicado serão considerados como data de término da correção.

4.49. Durante todo o período de execução dos serviços, a CONTRATADA é obrigada a manter, em base histórica, os dados sobre a execução de serviços em garantia.

**Requisitos de Experiência Profissional**

4.50. A experiência profissional necessária está detalhada em tópico específico deste Termo de Referência, no item 9.15 e seguintes.

**Requisitos de Segurança da Informação e Privacidade**

4.51. A Contratada deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.52. A contratada não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações da Prefeitura.

4.53. A contratada não poderá veicular publicidade acerca do fornecimento a ser contratada, sem prévia autorização, por escrito, da Prefeitura.

4.54. É de responsabilidade da contratada garantir a integridade e o sigilo das informações porventura contidas em equipamentos que sejam retirados das dependências da Prefeitura para realização de serviços de suporte técnico.

4.55. A contratada é responsável civil, penal e administrativa quanto à divulgação indevida ou não autorizada de informações, realizada por ela ou por seus empregados.

4.56. É de responsabilidade da contratada garantir que as informações por ela obtidas em decorrência da execução desta contratação sejam mantidas em sigilo, não podendo ser divulgadas, exceto se previamente acordado, por escrito, entre as partes contratantes.

4.57. Pertencerão exclusivamente à Prefeitura os direitos relativos aos serviços e artefatos (documentos etc.) desenvolvidos pelo CONTRATANTE durante a vigência do contrato, sendo vedada sua reprodução, transmissão e/ou divulgação sem o seu respectivo consentimento.

4.58. As informações constantes nos Relatórios de Chamados Técnicos e Relatórios de Nível de Serviço (RNS) serão de propriedade intelectual da Prefeitura, não devendo estas serem divulgadas sem o seu respectivo consentimento.

**Da exigência de carta de solidariedade**

4.59. Não será exigida carta de solidariedade emitida pelo fabricante.

**Da garantia da contratação**

4.60. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

4.61. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

**Subcontratação**

4.62. Não é admitida a subcontratação do objeto contratual.

**Requisitos de Metodologia de Trabalho**

4.63. O fornecimento dos equipamentos está condicionado ao recebimento pela Contratada de e-mail enviado pelo Contratante, indicando o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

4.64. A execução dos serviços de garantia está condicionada ao registro, na plataforma do fabricante, da ocorrência de falha no equipamento realizado pelo Contratante.

4.65. O registro na plataforma indicará o equipamento e a localidade na qual os serviços deverão ser prestados.

4.66. A contratada deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 07 dias por semana de maneira eletrônica e 08 horas por dia e 05 dias por semana (exceto sábado e domingo) por via telefônica.

4.67. A execução do serviço deve ser acompanhada pela Contratada, que dará ciência de eventuais acontecimentos ao Contratante.

**Da Prova Conceito (PoC) / Avaliação de Conformidade**

4.68. Havendo o aceite da proposta quanto ao valor, o interessado classificado provisoriamente em primeiro lugar deverá agendar junto à Secretaria Municipal de Tecnologia da Informação no prazo de até **03 (três)** dias úteis a demonstração prática das soluções, apresentando as funcionalidades requeridas neste Termo de Referência.

4.69. O prazo da apresentação deverá ocorrer em até **05 (cinco)** dias úteis após a divulgação do agendamento com a Secretaria Municipal de Tecnologia da Informação podendo eventualmente ser prorrogado mediante justificativa plausível e aceita pela mesma;

4.70. Após agendamento será informado no sistema do Portal de Compras Públicas, com no mínimo 24 horas de antecedência, o local, a data e hora da Prova de Conformidade (PoC), por meio de mensagem no ***chat*** do sistema, cuja presença será facultada a todos os interessados, incluindo os demais licitantes (devendo apresentar documento de identificação pessoal e procuração ou outro documento idôneo para comprovar os poderes e o interesse do licitante);

4.71. Não deverão ser feitos questionamentos durante as demonstrações, para que possa ser devidamente cumprido o prazo especificado para a apresentação, porém a licitante classificada em primeiro lugar deverá usar termo de referência como um checklist, demonstrando item a item;

4.71.1. Serão avaliados durante a demonstração os seguintes padrões mínimos de aceitabilidade:

4.71.1.1. Solução NGFW com IPS, controle de aplicações, VPN e autenticação multifator em alta disponibilidade - itens do 05 do Anexo I.a.;

4.71.1.2. Solução de política de segurança e autenticação à rede (NAC) - subitens do item 06 do Anexo I.a;

4.71.1.3. Solução de proteção de DNS recursivo - subitens do item 07 do Anexo I.a;

4.71.1.4. Solução de monitoramento de performance de aplicações - subitens do item 08 do Anexo I.a;

4.71.1.5. Solução de Monitoramento de experiência digita - subitens do item 09 do Anexo I.al;

4.71.1.6. Demonstrar atender a todos os objetivos e controles da NBR ISO/IEC 27.001 em sua versão mais recente dos itens do Anexo A, relacionados aos tópicos "A.6 - Controles de pessoas" e "A.8 - Controles tecnológicos", mediante apresentação de políticas, procedimentos, e outros documentos. Essa exigência não obriga a CONTRATADA a possuir a certificação ISO/IEC 27.001, mas sim demonstrar que possui os requisitos apropriados para tratar os dados da Prefeitura e atender o item 5.2.10 deste termo de referência.

4.72. Terminada a demonstração do sistema, a Administração, por meio do servidor responsável pelo setor correspondente, manifestar-se-á pela sua aprovação ou reprovação, sendo que, nesse último caso, deverá especificar as funcionalidades que entendeu não terem sido atendidas, ouvindo também eventuais apontamentos por parte das demais licitantes, que poderão se manifestar na ata ou incluir à ata um anexo constando os tópicos que entendeu oportuno se manifestar quanto aos não atendimentos;

4.73. Caso as demonstrações não sejam finalizadas no mesmo dia, poderá haver a continuidade no dia seguinte, lavrando-se em Ata as ocorrências até o momento da paralisação;

4.74. Será juntada aos autos as manifestações sobre o atendimento ou não das especificações contidas no Edital, sendo que o prazo para a manifestação de intenção de recurso será definido no Portal de Compras Públicas, conforme item 11 do Edital;

4.75. Se o(s) objeto(s) (solução) apresentada(s) através da PoC pelo primeiro classificado não for(em) aprovada(s), será analisada a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a demonstração do(s) objeto(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes neste Termo de Referência.

**Da vistoria técnica**

4.76. A vistoria prévia do local de execução dos serviços é **RECOMENDÁVEL** para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao fornecedor interessado o direito de sua realização;

4.76.1. A realização da vistoria **não se consubstancia em condição para a participação na licitação**.

4.77. O fornecedor que desejar realizar visita deverá agendar dia e horário específico, até o dia útil anterior à data limite do recebimento das propostas.

4.78. A vistoria será realizada nas seguintes condições:

4.78.1. Vedada a visita de mais de um fornecedor no mesmo momento;

4.79. A visita será agendada com o servidor Paulo Thame em dias úteis e seu agendamento se dará pelo telefone (11) 4622-7531 das 09:00h. às 16:00h. Responsável: Sr(a). Paulo Thame.

4.80. Alegações posteriores relacionadas com o desconhecimento de condições locais ou de projetos porventura disponibilizados, se for o caso, não serão consideradas para reclamações futuras, ou de forma a desobrigar a sua execução.

## 5. PAPÉIS E RESPONSABILIDADES

**5.1. São obrigações da CONTRATANTE:**

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. Receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

5.2. **São obrigações do CONTRATADO**

5.2.1. Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

5.2.9. Fazer a transição contratual, quando for o caso;

5.2.10. Garantir o cumprimento de normativos internacionais de boas práticas da família ISO/IEC 20000 e

ISO/IEC 27000, em sua versão mais recente.

## 6. MODELO DE EXECUÇÃO DO CONTRATO

6.1.1. O gestor do contrato emitirá a ORDEM DE FORNECIMENTO para a entrega dos bens desejados.

6.1.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na ORDEM DE FORNECIMENTO.

6.1.3. O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio deste TR.

**Forma de execução e acompanhamento do contrato**

**Condições de Entrega**

6.1.4. O prazo de entrega dos bens é de 90 dias, contados do(a) recebimento da Ordem de Fornecimento, em remessa única

6.1.5. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 05 (cinco) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

**Local e horário da prestação dos serviços**

6.1.6. Os bens deverão ser entregues no endereço da Prefeitura na Avenida Marechal Mascarenhas de Moraes, 1283 – Sítio do Morro – Santana de Parnaíba/SP - CEP: 06517-520, na Secretaria Municipal de Tecnologia da Informação (SMTI).

6.1.7. Todos os serviços realizados presencialmente deverão ser realizados no mesmo endereço do item anterior.

**Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)**

6.1.8. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo, 48 (quarenta e oito) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

6.1.9. A PREFEITURA poderá solicitar a revisão sobre os resultados entregues na realização dos serviços que tenham sido feitos fora do escopo acordado no Contrato e/ou das normas, padrões, procedimentos e instruções técnicas da PREFEITURA, ou ainda em desacordo com a legislação vigente, ficando a CONTRATADA obrigada a refazer o serviço conforme obrigação estabelecida neste Contrato, sem ônus para a PREFEITURA.

6.1.10. Todo resultado entregue a partir dos serviços realizados pela CONTRATADA terá garantia de correções e ajustes necessários durante os 90 (noventa) dias seguintes à conclusão daqueles serviços, mesmo que essa conclusão tenha ocorrido nos últimos 90 (noventa) dias do Contrato.

6.1.11. Dentro do período de garantia, a correção de erros nos serviços entregues pela CONTRATADA deverá ser efetuada sem qualquer ônus para a PREFEITURA, seja financeiro ou de atraso na prestação de outro(s) serviço(s), desde que, comprovadamente, não tenham se dado em razão das especificações feitas pela PREFEITURA.

6.1.12. A garantia do produto é estabelecida considerando-se a versão de Software entregue e futuras

versões de Software.

6.1.13. A correção deverá ser executada pela CONTRATADA no prazo máximo de 24 (vinte e quatro) horas úteis, contadas a partir do comunicado feito pela PREFEITURA junto à CONTRATADA sobre o defeito encontrado.

6.1.14. Extinta a vigência do CONTRATO, a CONTRATADA terá 05 (cinco) dias úteis para atendimento.

6.1.15. Caso a CONTRATADA entenda necessária, em um serviço específico, a dilatação dos prazos definidos, deverá justificar-se tecnicamente por meio de relatório formal.

6.1.16. Caso a PREFEITURA não aceite as argumentações, não haverá interrupção na contagem do prazo definido previamente.

6.1.17. A não observância ao prazo para correção de defeito implica na aplicação das penalidades cabíveis.

6.1.18. Terminada a correção pertinente, a CONTRATADA enviará para o responsável pelo(s) artefato(s), designado pela PREFEITURA, com cópia para a Gestão do Contrato, o(s) artefato(s) corrigido(s). A data e hora do envio deste comunicado serão considerados como data de término da correção.

6.1.19. Durante todo o período de execução dos serviços, a CONTRATADA é obrigada a manter, em base histórica, os dados sobre a execução de serviços em garantia.

**Formas de transferência de conhecimento**

6.1.20. A CONTRATADA deverá prestar serviços de Treinamentos para equipe da PREFEITURA conforme os conteúdos mínimos indicados a seguir com o intuito de assegurar a transferência de conhecimento.

6.1.20.1. Solução de firewall de próxima geração com ips, controle de aplicações, vpn e autenticação multifator:

6.1.20.1.1. O Treinamento não-oficial (ou repasse de conhecimento) deverá ser ministrado nas dependências da PREFEITURA, de forma online, ou nas dependências da CONTRATADA sobre as Soluções de Firewall, Gerência, MFA e solução de VPN;

6.1.20.1.2. As despesas decorrentes do serviço de Treinamento (instrutores, confecção do material didático) serão de exclusiva responsabilidade da CONTRATADA;

6.1.20.1.3. O instrutor deverá ser certificado na solução ofertada.

6.1.20.1.4. O treinamento não oficial deverá ter a carga horária mínima de 40 (quarenta) horas.

6.1.20.1.5. O Treinamento poderá ser ministrado para até quatro colaboradores indicados pela PREFEITURA.

6.1.20.1.6. A CONTRATADA também deverá fornecer, além do treinamento não-oficial, o Treinamento OFICIAL de FABRICANTE com duração de pelo menos 40 horas para até três colaboradores para o NGFirewall e VPN, indicados pela PREFEITURA, nas instalações de um centro autorizado pelo fabricante, na cidade de São Paulo, sujeito a disponibilidade de turma.

6.1.20.1.7. Ao final do treinamento deverá ser emitido certificado de conclusão para cada aluno que concluir o curso.

6.1.20.2. Solução de política de segurança e autenticação à rede (nac)

6.1.20.2.1. O Treinamento não-oficial (ou repasse de conhecimento) deverá ser ministrado nas dependências da PREFEITURA sobre as Solução de Network Admission Control (NAC);

6.1.20.2.2. As despesas decorrentes do serviço de Treinamento (instrutores, confecção do material didático) serão de exclusiva responsabilidade da CONTRATADA;

6.1.20.2.3. O instrutor deverá ser certificado na solução ofertada.

6.1.20.2.4. O treinamento deverá ter a carga horária mínima de 40 (quarenta) horas.

6.1.20.2.5. O Treinamento poderá ser ministrado para até quatro colaboradores indicados pela PREFEITURA.

6.1.20.2.6. A CONTRATADA também deverá fornecer, além do treinamento não-oficial, o Treinamento OFICIAL de FABRICANTE com duração de pelo menos 40 (quarenta) horas para até três colaboradores para a Solução de NAC, indicados pela PREFEITURA, nas instalações de um centro autorizado pelo fabricante, na cidade de São Paulo, sujeito a disponibilidade de turma.

6.1.20.2.7. Ao final do treinamento deverá ser emitido certificado de conclusão para cada aluno que concluir o curso.

6.1.20.3. Solução de proteção de dns recursivo

6.1.20.3.1. O Treinamento oficial do fabricante deverá ser ministrado nas dependências da PREFEITURA de forma online ou nas dependências da CONTRATADA sobre a Solução de proteção de dns recursivo;

6.1.20.3.2. As despesas decorrentes do serviço de Treinamento (instrutores, confecção do material didático) serão de exclusiva responsabilidade da CONTRATADA;

6.1.20.3.3. O instrutor deverá ser certificado na solução ofertada.

6.1.20.3.4. O treinamento deverá ter a carga horária mínima de 24 (vinte e quatro) horas.

6.1.20.3.5. O Treinamento poderá ser ministrado para até quatro colaboradores indicados pela PREFEITURA.

6.1.20.3.6. Ao final do treinamento deverá ser emitido certificado de conclusão para cada aluno que concluir o curso.

6.1.20.4. Solução de monitoramento de performance de aplicações e monitoramento de experiência digital

6.1.20.4.1. O Treinamento não-oficial (ou repasse de conhecimento Hands-on) deverá ser ministrado remotamente a equipe da PREFEITURA sobre a Solução de Performance de Aplicação, com no mínimo 24 (vinte e quatro) horas de duração;

6.1.20.4.2. O(s) instrutor(es) deverá(ão) ser certificado nas soluções ofertadas;

6.1.20.4.3. O Treinamento poderá ser ministrado para até quatro colaboradores indicados pela PREFEITURA.

6.1.20.4.4. A CONTRATADA também deverá fornecer, além do treinamento não-oficial, o Treinamento OFICIAL de FABRICANTE com duração de pelo menos 40 horas para no mínimo 08 (oito) colaboradores, sendo realizados em até 2 turmas, com 04 (quatro) alunos cada, uma no período matutino e outra no período vespertino.

6.1.20.4.5. As despesas decorrentes do serviço de Treinamento (instrutores, confecção do material didático) serão de exclusiva responsabilidade da CONTRATADA;

6.1.20.4.6. É obrigatório um mínimo de 40 (quarenta) horas úteis de carga horária para cada turma;

6.1.20.4.7. Os treinamentos deverão ser divididos em módulos de 4 (quatro) horas diárias e, deverão ser ministrados em dois turnos, com uma turma no período matutino e outra no período vespertino, conforme a necessidade da PREFEITURA, em horário comercial e dias úteis contínuos;

6.1.20.4.8. A capacitação deve ser realizada em dias úteis, de segunda a sexta-feira, em horário comercial entre 08:00 e 18:00, em datas previamente acordadas pelas partes;

6.1.20.4.9. O Treinamento poderá ser ministrado online ou nas instalações da CONTRATADA para até quatro

colaboradores indicados pela PREFEITURA.

6.1.20.4.10. Ao final do treinamento deverá ser emitido certificado de conclusão para cada aluno que concluir o curso.

**Mecanismos formais de comunicação**

6.1.21. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:

6.1.21.1. E-mail;

6.1.21.2. Ordem de Serviço;

6.1.21.3. Sistema de abertura de chamados;

6.1.21.4. Ata de Reunião;

6.1.21.5. Ofício;

## 7. MODELO DE GESTÃO DO CONTRATO

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

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

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

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

**Reunião Inicial**

7.5. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

7.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10 (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.6.1. A pauta desta reunião observará, pelo menos:

7.6.1.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.6.1.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.6.1.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.6.1.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais

questões técnicas, legais e administrativas referentes ao andamento contratual;

7.6.1.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

**Fiscalização**

7.7. A fiscalização do objeto será exercida pela SMTI da PMSP, que deverá controlar e avaliar em conformidade com as exigências do Edital;

7.8. Qualquer exigência da fiscalização, respaldada na legislação aplicável, no Edital e seus anexos e no Contrato, deverá ser imediatamente atendida pela CONTRATADA;

7.9. Incumbe à fiscalização verificar se o fornecimento dos materiais, equipamentos e/ou serviços estão de acordo com as exigências do Edital e seus anexos;

7.10. As exigências formuladas são mínimas e regem cada caso, devendo prevalecer sempre as Normas Brasileiras, Regulamentos, Posturas Municipais, Estaduais, Federais, Normas dos Fabricantes e das operadoras de eletricidade e de telecomunicações ou aquelas que apresentarem exigências mais rigorosas ou forem mais recentes e atualizadas;

7.11. Estando em conformidade com as especificações do Edital e seus anexos, os documentos correspondentes de cobrança deverão ser examinados e atestados pela fiscalização da SMTI e enviados ao Tesouro Municipal para pagamento;

7.12. No caso de recusa da fiscalização em atestar a nota fiscal/fatura ou documento similar, relativo a entrega do objeto deste Termo de Referência, a CONTRATADA será notificada, por escrito, sobre as irregularidades apontadas pelo fiscal, para adoção de providências conforme artigo 119 da lei nº 14.133/2021, no que couber;

7.13. A supervisão por parte da CONTRATANTE, sob qualquer forma, não isenta ou diminui a responsabilidade da CONTRATADA na perfeita execução do objeto contratual.

7.14. Gestor do Contrato: André da Quinta Vieira, prontuário 28.613.

7.15. Fiscal Técnico: Paulo Carvalho Thame, prontuário 36.990.

7.16. Fiscal Administrativo: Marta Ribeiro Amaral, prontuário 41.026.

## 8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

**Critérios de Aceitação**

8.1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados nos tópicos a seguir.

8.2. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

8.3. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes

que sejam fisicamente ou logicamente incompa]veis.

8.4. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

8.5. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

8.6. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

8.7. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

8.8. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas) ou em modo de subscrição, legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

8.9. A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

8.10. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

8.11. Após o aceite definitivo, a Secretaria Municipal de Tecnologia da Informação (SMTI) seguirá com o envio da fatura/nota fiscal ou documento similar ao Tesouro Municipal.

8.12. Quando for constatada qualquer irregularidade na fatura/nota fiscal ou documento similar, será imediatamente solicitada à CONTRATADA carta de correção quando couber, ou ainda pertinente regularização, que deverá ser encaminhada à CONTRATANTE através do e-mail smti.notafiscal@santanadeparnaiba.sp.gov.br, no prazo de 24 (vinte quatro) horas;

8.13. A CONTRATADA deverá enviar o documento fiscal, após o recebimento definitivo e o arquivo de Nota Fiscal por XML, para os e-mails para smti.notafiscal@santanadeparnaiba.sp.gov.br e nfe@santanadeparnaiba.sp.gov.br.

8.14. Caso a CONTRATADA não apresente carta de correção no prazo estipulado, o prazo para pagamento será contado a partir da data da sua apresentação.

**Procedimentos de Teste e Inspeção**

8.15. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

8.15.1. Inspeção/teste dos componentes Físicos e lógicos;

8.15.2. Inspeção/teste da configuração inicial da solução, incluindo a interface de gerenciamento e configurações básicas;

8.15.3. Inspeção/teste da configuração de políticas de segurança, incluindo filtragem de conteúdo, controle de aplicativos e regras de firewall;

8.15.4. Inspeção/teste da aplicabilidade de políticas personalizadas para atender às necessidades específicas da instituição;

**Níveis Mínimos de Serviço Exigidos**

8.16. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

| IAP – ÍNDICE DE ATENDIMENTO NO PRAZO | |
|---|---|
| Tópico | Descrição |
| Finalidade | Medir o tempo de atraso na prestação dos serviços constantes na Ordem de Fornecimento. |
| Meta a cumprir | IAP A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento dentro do prazo previsto |
| Instrumento de medição | Ordem de Fornecimento, Termo de Recebimento Provisório (TRP) |
| Forma de acompanhamento | É apurado pelos fiscais do contrato avaliando a quantidade atendida dentro do prazo em relação à quantidade total atendida no período de referência. |
| Periodicidade | Mensal |

| | |
|---|---|
| Mecanismo de Cálculo (métrica) | IAP = 100 * (ΣQtap / ΣQtr)<br><br>Onde:<br>IAP = Indicador de atendimento aos prazos do serviço;<br>ΣQtap = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência;<br>ΣQtr = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência. |
| Observações | Obs1: Serão utilizados dias corridos na medição.<br>Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador. |
| Início de Vigência | A partir da emissão da OS. |
| Faixas de ajuste no pagamento e Sanções | IAP >= 90%: sem descontos sobre o valor da fatura mensal.<br>IAP >= 80% e < 90%: 5% de desconto sobre o valor da fatura mensal.<br>IAP >= 70% e < 80%: 7% de desconto sobre o valor da fatura mensal.<br>IAP < 70%: 9% de desconto sobre o valor da fatura mensal. |

8.17. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

8.17.1. não produzir os resultados acordados;

8.17.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas;

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

**Liquidação**

8.19. O pagamento da instalação e configuração da solução será realizado em parcela única

8.20. Os itens que fazem parte deste Termo de Referência serão pagos em parcela fixa mensalmente durante 48 (quarenta e oito) meses, em até 30 (trinta) dias contados da comprovada apresentação da respectiva documentação fiscal, devidamente atestada pela SMTI após a instalação completa da solução.

**Prazo de pagamento**

8.21. O pagamento será efetuado no prazo de **até 30 (trinta) dias corridos** contados da finalização da liquidação da despesa, conforme seção anterior.

**Forma de pagamento**

8.22. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo FORNECEDOR.

8.23. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.24. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.25. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.26. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

**Antecipação de pagamento**

8.27. A presente contratação **NÃO** permite a antecipação de pagamento

**Cessão de crédito**

8.28. Não se aplica à antecipação de pagamento parcial ou total à presente contratação.

## 9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

9.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo **menor preço**.

**Regime de execução**

9.2. O fornecimento do objeto será integral.

**Da Aplicação da Margem de Preferência**

9.3. Considerando o disposto no item 1.6, e para fins de participação nesta licitação, justificada a impossibilidade e inviabilidade de atendimento dos artigos 47 a 48 da LC 123/06 e alterações, o certame será aberto para competição de todas as empresas que atenderem às exigências deste edital, e, **não serão reservadas cotas ou subcontratações para MPEs**, à exceção da observação do direito de preferência em caso de empate ficto, e da regularidade fiscal e trabalhista postergadas que se aplicam integralmente às beneficiadas..

**Exigências de habilitação**

9.4. Para fins de habilitação, deverá o licitante apresentar os documentos previstos no ANEXO IV - RELAÇÃO DE DOCUMENTOS DE HABILITAÇÃO, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação.

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

exigências que deverão ser complementadas observando sempre as regras dispostas no edital.

**QUALIFICAÇÃO TÉCNICA**

9.6. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

9.7. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

9.7.1. Pelo menos um Atestado de Capacidade Técnica de serviço de suporte a Soluções;

9.7.2. Pelo menos um Atestado de Capacidade Técnica de serviço de Consultoria na área de Segurança da informação;

9.7.3. Pelo menos um Atestado de Capacidade técnica consolidando no mesmo Atestado os serviços os seguintes serviços de SOC:

9.7.3.1. Serviços Gerenciados de segurança para: Firewall e NAC.

9.7.3.2. Serviço de CSIRT.

9.7.4. Atestado de Capacidade Técnica de Proteção de DNS (DNS recursivo), para um mínimo de 3000 usuários;

9.7.5. Atestado de Capacidade Técnica de Solução de Política e Autenticação a Rede (NAC), para ambiente com no mínimo de 3.000 dispositivos.

9.7.6. Atestados de Capacidade Técnica de Monitoração de Performance de aplicação.

9.7.7. Pelo menos um Atestado de Capacidade Técnica de Serviço de sustentação, administração e monitoramento de ambientes tecnológicos complexos, com mais de 3.000 dispositivos e tecnologias de fabricantes distintos envolvidas com, no mínimo, 5.000 horas comprovadas de prestação de serviço em regime 24x7;

9.8. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados, 9.7.4, 9.7.5 e 9.7.7 deverão ser de forma concomitante.

9.9. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

9.10. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

9.11. **Declarações da licitante:** elaborada em papel timbrado e subscrita por seu representante legal, expressando que está devidamente credenciada e capacitada para comercializar os equipamentos e softwares que compõem toda a solução, e ainda, que faz parte do programa de parceiros do fabricante da solução. Aplicável caso a empresa não possua no momento da habilitação a declaração do fabricante.

9.11.1. A declaração busca identificar, por meio do documento emitido pelo fabricante, que os produtos/ serviços fornecidos pela CONTRATADA têm assegurada a sua procedência e qualidade, bem como assevera também que o treinamento dos técnicos designados pela PREFEITURA e o

suporte técnico pós-implantação da solução, serão prestados com emprego de profissionais qualificados e habilitados na tecnologia empregada pela fabricante.

9.11.2. São elementos essenciais para garantir a plena operabilidade da solução, em regime de redundância, independentemente de disfunções detectadas no ambiente, assegurando a continuidade das atividades dos usuários das Entidades, suportadas pelos processos de TI.

9.12. A CONTRATADA, para atendimento das exigências acima, deve apresentá-las antes da assinatura do Contrato.

**Da participação de cooperativas**

9.13. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

9.13.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

9.13.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

9.13.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

9.13.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

9.13.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

9.13.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

9.13.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

**PROPOSTA TÉCNICA (ANEXO V)**

9.14. A CONTRATADA deverá apresentar obrigatoriamente emitir documento de emissão própria, em papel timbrado, descrevendo sua estratégia para atendimento aos requisitos da Proposta Técnica. Deverão ser fornecidas as seguintes informações a respeito:

9.14.1. Detalhe das Soluções e Serviços empregados: Detalhamento e descrição de cada uma dos equipamentos, softwares e demais recursos técnicos, além dos partnumbers (SKU´s), quantitativos, links dos datasheets das soluções, duração de suporte a serem fornecidos ou alocados ao serviço, com os devidos tempos de duração e SLAs.

9.14.2. Plano e Cronograma de Implantação das Soluções: completo, em formato eletrônico, nos termos exigido neste Memorial, contendo:

9.14.2.1. Escopo de implementação com Matriz de responsabilidade.

9.14.2.2. Estrutura Analítica do Projeto (WBS – Work Breakdown Structure).

9.14.2.3. Cronograma de atividades apresentado, demonstrando as dependências e os marcos, observando-se os prazos definidos.

9.14.2.4. Plano de treinamento (Hands-on).

9.14.2.5. Testes e critérios de aceitação.

9.14.2.6. Detalhamento da Estrutura do Atendimento do Serviço Gerenciado, demonstrando o processo de gerenciamento de mudanças sobre as tecnologias existentes e soluções adquiridas como serviço pela PREF. STA. PARNAÍBA, um resumo das atividades de mudanças a ser executadas nos produtos, bem como os SLAs comprovando os níveis de serviço requisitados pela PREFEITURA.

9.14.2.7. Detalhamento da Estrutura de atendimento de Suporte Técnico e demais processos.

**QUALIFICAÇÕES TÉCNICAS PROFISSIONAIS**

9.15. **Declaração da licitante**, elaborada em papel timbrado e subscrita por seu representante legal, de que possui os profissionais devidamente qualificados para a execução do objeto licitado, conforme legislação vigente ou Declaração de Contratação futura, caso a empresa não possua o profissional com a qualificação exigida no momento da habilitação, a saber:

**GRUPO SERVIÇOS TÉCNICOS CONTINUADOS DE SOLUÇÕES CISCO E WIFI**

9.16. **PROFISSIONAL EXPERT – ESPECIALIZAÇÃO DE REDES**

9.16.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

9.16.2. Certificação:

9.16.2.1. Cisco Certified Certification Internetwork Expert – CCIE Routing & Switching válido.

9.16.3. Experiência:

9.16.3.1. Experiência mínima de 05 (cinco) anos comprovada em Troubleshooting de em Ambientes de Redes;

9.16.3.2. Conhecimento em Redes Avançado para implantação e Troubleshooting envolvendo Firewalls, Ambientes com NAC, Proteção a DNS recursivo e demais produtos de cibersegurança.

9.17. **PROFISSIONAL SÊNIOR – ESPECIALIZAÇÃO DE REDES WIRELESS CISCO**

9.17.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

9.17.2. Certificação:

9.17.2.1. Cisco Certified Certification Internetwork Expert – CCNP Wireless válido.

9.17.3. Experiência:

9.17.3.1. Experiência mínima de 03 (três) anos comprovada em Troubleshooting de em Ambientes de Redes;

**GRUPO DE SERVIÇOS GERENCIADOS DE SEGURANÇA:**

9.18. **PROFISSIONAL EXPERT – ESPECIALIZAÇÃO CIBERSEGURANÇA**

9.18.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

9.18.2. Certificação:

9.18.2.1. Checkpoint Certified Security Expert (CCSE) ou Cisco Certified Certification Internetwork Expert – CCIE Security ou Fortinet Network Security Expert (NSE8) válido.

9.18.3. Experiência:

9.18.3.1. Experiência mínima de 05 (cinco) anos comprovada em Troubleshooting de em Ambientes Cibersegurança;

9.18.3.2. Conhecimento em Redes Avançado para implantação e Troubleshooting envolvendo Firewalls, Ambientes com NAC, Proteção a DNS recursivo e demais produtos de cibersegurança.

9.19. **PROFISSIONAL DE SEGURANÇA SÊNIOR – SOLUÇÃO DE NAC**

9.19.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

9.19.2. Certificação:

9.19.2.1. Certificação Aruba Certified ClearPass Expert (ACCX) ou Cisco CCNP Security

9.19.3. Experiência:

9.19.3.1. Experiência mínima de 05 (cinco) anos comprovada em Operação Avançada e Troubleshooting, Consultoria em Ambientes com Solução NAC.

9.20. **ANALISTA DE SEGURANÇA PARA SOLUÇÃO DE MFA (MULTIPLO FATOR DE AUTENTICAÇÃO)**

9.20.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

9.20.2. Certificação:

9.20.2.1. CompTIA Security+ ou Certificação sobre a plataforma/solução utilizada.

9.20.3. Experiência:

9.20.3.1. Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado;

9.20.3.2. Experiência comprovada de no mínimo 02 (dois) anos em segurança da informação.

9.21. **GESTOR DO CENTRO DE OPERAÇÃO DE SEGURANÇA**

9.21.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação ou de Segurança da informação, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).

9.21.2. Descrição:

9.21.2.1. Elaborar documentação de processos.

9.21.2.2. Ser responsável por alinhar operações táticas de segurança à estratégia de negócios da PREFEITURA e seus clientes;

9.21.2.3. Elaborar documentação de padrões de segurança;

9.21.2.4. Realçar políticas de segurança da informação;

9.21.2.5. Criar a matriz de responsabilidade e funções;

9.21.2.6. Apoiar na aplicação de políticas de segurança e domínios de segurança;

9.21.2.7. Desenvolver programa de classificação e propriedade dos dados tratados;

9.21.2.8. Criar os planos de resposta a incidentes;

9.21.2.9. Criar os planos de continuidade de negócios;

9.21.2.10. Participar de reuniões de alinhamento sobre os processos e estratégias de segurança;

9.21.2.11. Conduzir entrevistas e assessments de maturidade para identificar o estado atual dos itens que compõe a segurança cibernética da PREFEITURA;

9.21.2.12. Apresentar os resultados obtidos, além de propor melhorias no estado de maturidade de segurança cibernética da PREFEITURA.

9.21.3. Certificação:

9.21.3.1. ISACA Certified Information Security Manager (CISM) válido;

9.21.4. Experiência:

9.21.4.1. Experiência mínima de 05 (cinco) anos comprovada no setor de segurança cibernética, em coordenação e gestão de contratos de serviços continuados.

9.22. **GERENTE DE PROJETOS DE TI SÊNIOR**

9.22.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Project Management Professional (PMP). Professional Scrum Master I.

9.22.2. Descrição:

9.22.2.1. Soft Skills (organização, liderança, comunicação, negociação, visão holística, alocação de recursos, gestão de crises, objetividade, empatia e disciplina).

9.22.2.2. Conhecimento avançado teórico e prático em gerenciamento de projetos (PMI), COBIT e ITIL;

9.22.2.3. Conhecimento da norma ISO/IEC 27001;

9.22.2.4. Implantação, gerenciamento de atividades e gestão de equipe utilizando metodologias ágeis scrum e kanban que façam parte do escopo de gestão da CONTRATADA;

9.22.2.5. Elaborar documentações pertinentes ao escopo de gestão de projeto como cronogramas, matriz de comunicação, atas de reunião, relatórios de implantação e organogramas;

9.22.2.6. Apoiar no gerenciamento do plano de ações de remediação e mitigação para todas as soluções que façam parte do escopo da CONTRATADA de monitoração e gestão;

9.22.2.7. Apoiar no gerenciamento do plano de remediar e mitigar riscos nas soluções que façam parte do escopo de gestão da CONTRATADA.

9.23. Certificação:

9.23.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de Gestão de projetos;

9.23.2. Certificações em SCRUM ou PMI.

9.24. Experiência:

9.24.1. Conhecimento de arquiteturas;

9.24.2. Conhecimento prático sobre atuação utilizando metodologias ágeis;

9.24.3. Vivência em implantação de práticas de PMO e QA em projetos;

9.24.4. Experiência com agile e uso desta abordagem;

9.24.5. Experiência mínima de 5 (cinco) anos comprovada no setor de gestão de projetos, preferencialmente em segurança cibernética, com prática em powerBI, elaboração de atas de reunião, condução de reuniões de alinhamento, elaboração de cronogramas em Microsoft Project, elaboração de matriz de comunicações e documentações pertinentes ao escopo de gestão de projetos.

**GRUPO DE RESPOSTA A INCIDENTE CIBERNÉTICOS, da CONTRATADA são:**

9.25. **ANALISTA DE SEGURANÇA I - LINUX LPIC 1 OU ISFS (INFORMATION SECURITY FOUNDATION)**

9.25.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

9.25.2. Certificação:

9.25.2.1. Especializações na área de segurança da informação.

9.25.2.2. Conhecimento avançado em segurança da informação, com experiência em resposta a incidente de segurança da informação.

9.25.3. Experiência:

9.25.3.1. Experiência comprovada de no mínimo 2 (dois) anos em segurança da informação.

9.26. **ANALISTA DE SEGURANÇA II - CERTIFIED ETHICAL HACKER**

9.26.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

9.26.2. Certificação:

9.26.2.1. Especializações na área de segurança da informação.

9.26.2.2. Conhecimento avançado em segurança da informação, com experiência em resposta a incidente de segurança da informação.

9.26.3. Experiência:

9.26.3.1. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

9.27. **ANALISTA DE SEGURANÇA III - COMPTIA SECURITY+ OU CERTIFIED ETHICAL HACKER**

9.27.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

9.27.1.1. Certificação:

9.27.1.1.1. Especializações na área de segurança da informação.

9.27.1.1.2. Conhecimento avançado em segurança da informação, com experiência em resposta a incidente de segurança da informação.

9.27.1.2. Experiência:

9.27.1.2.1. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

9.28. **ANALISTA DE SEGURANÇA III - CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL**

9.28.1. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

9.28.2. Certificação:

9.28.2.1. Certificação CISSP - Certified Information Systems Security Professional válida

9.28.2.2. Conhecimento avançado em segurança da informação, com experiência em resposta a incidente de segurança da informação

9.28.3. Experiência:

9.28.3.1. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

9.29. As provas e certificações solicitadas deverão estar dentro do prazo de validade durante toda a duração do contrato.

9.30. A CONTRATADA, para atendimento das exigências acima e das demais descritas em edital, deve apresentá-las antes da assinatura do Contrato.

9.31. A Comprovação do vínculo do profissional para atendimento dos itens descritos acima, mediante Contrato Social, registro na Carteira Profissional, Ficha de Empregado ou Contrato de Trabalho, sendo possível a contratação de profissional autônomo que preencha os requisitos e se responsabilize tecnicamente pela execução dos serviços ou de documentos equivalentes, nos termos admitidos pela Súmula 25 do TCE-SP.

9.32. **AMBIENTE DA CONTRATADA - CENTROS DE OPERAÇÕES DE SEGURANÇA**

9.32.1. Preenchimento do ANEXO I.b - Requisitos de Atendimento do SOC

9.32.2. Todos os serviços gerenciados devem ser providos através de Centro de Operações de Segurança (Security Operation Center - SOC), incluindo minimamente 02 (dois) ambientes na CONTRATADA, redundantes entre si e distantes, com pelo menos, 20 km de distância geodésica um do outro.

9.32.3. Devido a necessidade de atendimento presencial, nos diversos serviços contratados, sob demanda e solicitado através de requisições de serviço, pelo menos um destes Centros de Operação de Segurança deve estar localizado no Estado de São Paulo. Além disso, pelo menos 01 (um) dos SOCs deverá estar a no máximo 40 km de distância da PREFEITURA DE SANTANA DE PARNAÍBA, para permitir a participação da CONTRATADA em “War Room” ou salas de crise, conforme consta no Anexo II – REQUISITOS DE ATENDIMENTO DO SOC.

9.32.4. Os 02 (dois) Centros de Operações de Segurança (SOC) já devem estar em pleno funcionamento na data da diligência, exigido na licitação, redundantes, de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados.

9.32.5. Devem ser configurados de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços.

9.32.6. A CONTRATADA deverá fornecer links de comunicação dedicados, para interligação de seu ambiente ao ambiente da PREFEITURA, cuja utilização não deverá ultrapassar 90% (noventa por cento) de sua capacidade. Podendo ser utilizado VPN via internet como redundância.

9.32.7. Recursos físicos da CONTRATADA (prédio, salas, mesas e outros) poderão ser compartilhados com outros clientes, desde que:

9.32.8. Toda a infraestrutura lógica que atende a PREFEITURA seja separada dos demais clientes;

9.32.9. As estações de trabalho sejam segmentadas por VLANs e/ou controle compensatório de segurança;

9.32.10. Todos os funcionários possuam assinado um documento de termo de responsabilidade e sigilo, conforme ANEXO I.c. - TERMO DE CONFIDENCIALIDADE E PROTEÇÃO DE DADOS.

9.32.11. A CONTRATADA será responsável pela aplicação de controles de segurança adequados (criptografia) para garantir a confidencialidade de qualquer dado ou informação do PREFEITURA que receber em seu ambiente ou em terceiro contratado.

9.32.12. A CONTRATADA deverá comunicar formalmente a PREFEITURA sempre que identificar algum serviço com falhas de implementação e que tornem o ambiente vulnerável à indisponibilidade.

## 10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado da contratação para o(s) item(ns) / lote(s) é o que consta no ANEXO III - PLANILHA DE ITENS E VALORES ESTIMADOS que compõe o Edital.

10.2. As condições para alteração ou atualização em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, são as descritas no ANEXO VI - MINUTA DE TERMO DE CONTRATO.

## 11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no orçamento municipal.

11.2. A contratação será atendida pela(s) seguinte(s) funcional(is) programática(s):

11.2.1. Secretaria Municipal de Tecnologia da Informação – SMTI

11.2.2. Fonte de Recurso: Tesouro Municipal

11.2.3. Funcional Programática: nº 0209-3.3.90.40-0412200152026

11.2.4. Reserva nº 2440

**Equipe Técnica Responsável pela elaboração do Termo de Referência (TR)**

gov.br Documento assinado digitalmente
PAULO CARVALHO THAME
Data: 06/05/2024 10:11:14-0300
Verifique em https://validar.iti.gov.br

**Paulo Thame**
Lider Data Center
Prontuário: 36.990

gov.br Documento assinado digitalmente
JOSE ROBERTO CAMPOS DE SIQUEIRA
Data: 06/05/2024 10:42:32-0300
Verifique em https://validar.iti.gov.br

**José Roberto Campos de Siqueira**
Coordenador Operacional
Prontuário: 32.888

gov.br Documento assinado digitalmente
FELIPE CREMM
Data: 06/05/2024 10:21:34-0300
Verifique em https://validar.iti.gov.br

**Felipe Cremm**
Coordenador de Desenvolvimento
Prontuário: 30.777

**ANEXO I.a.**

**ESPECIFICAÇÕES DETALHADAS**

## 1. SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES

### 1.1. REQUISITOS DE NEGÓCIO

1.1.1. A empresa PREFEITURA, com objetivo de melhorar sua maturidade em segurança cibernética, busca serviço de empresa para parceria estratégica de segurança, onde este possa ser capaz de realizar escopo bastante diversificado de múltiplas atividades de segurança.

1.1.2. A PREFEITURA busca serviço de gestão dos ativos de segurança, considerando a sua arquitetura de tecnologia. Devem ser consideradas todas ferramentas de segurança adquiridas pela PREFEITURA para realização da gestão dos dispositivos.

1.1.3. Os serviços gerenciados a serem fornecidos pela CONTRATADA deverão ser realizados no regime 24x7x365 e possuem site de operação backup em localidade diferente do site principal.

1.1.4. Conforme definição da PREFEITURA, a CONTRATADA deverá ser responsável pelas seguintes atividades a serem descritas neste documento:

1.1.4.1. Serviço gerenciado de soluções de segurança (Administração de soluções de segurança).

1.1.5. Esta contratação terá 48 (quarenta e oito) meses de duração.

### 1.2. PRINCIPAIS CARACTERÍSTICAS

1.2.1. O serviço gerenciado deve oferecer serviços personalizados para transformar as operações de segurança. Deve gerenciar, manter e monitorar de forma proativa os dispositivos de segurança e aumentar a visibilidade de ameaças com a análise avançada de tráfego de rede.

1.2.2. A PREFEITURA espera que a CONTRATADA entregue este serviço por engenheiros certificados e analistas de segurança experientes 24 horas por dia, 7 dias por semana.

1.2.3. O serviço gerenciado que a PREFEITURA espera ter deve fornecer:

1.2.3.1. Gerenciamento das plataformas, incluindo monitoramento de saúde e disponibilidade, aplicação de patch, manutenção de sistema operacional, backup e restauração.

1.2.3.2. Monitoramento de conformidade, relatórios e notificações com base nos requisitos da PREFEITURA;

1.2.3.3. Integração com a equipe de Segurança da PREFEITURA, para transferência de conhecimento.

1.2.3.4. Fornecimento de soluções com manutenção e suporte técnico durante todo o período do contrato:

1.2.3.4.1. Fornecimento de solução firewall de próxima geração com IPS, controle de aplicações, VPN e autenticação multifator em alta disponibilidade

1.2.3.4.2. Fornecimento de solução de política de segurança e autenticação à rede (NAC)

1.2.3.4.3. Fornecimento de solução de proteção de DNS recursivo

1.2.3.5. O detalhamento técnico das soluções, características de manutenção e suporte técnico estão descritos neste documento.

### 1.3. SOLUÇÕES COMO SERVIÇO SEM O GERENCIAMENTO DA CONTRATADA

1.3.1. As seguintes soluções serão adquiridas pela PREFEITURA no modelo de Solução como Serviço, aonde a PREFEITURA fica responsável pela gestão das soluções e a CONTRATADA responsável somente pela instalação, suporte técnico e garantia das mesmas:

1.3.1.1. Fornecimento de Solução de monitoramento de performance de aplicações;

1.3.1.2. Fornecimento de Solução monitoramento de experiência digital.

1.3.2. Para eventuais serviços de implementação não previstos na instalação das soluções, a PREFEITURA fará uso de Banco de horas sob demanda previamente adquirido da CONTRATADA.

1.4. **ELEMENTOS PRINCIPAIS DO SERVIÇO**

1.4.1. **HORÁRIO DE OPERAÇÃO**

1.4.1.1. Os Serviços Gerenciados de Segurança deverão ser fornecidos por meio dos Centros de Operações de Segurança da CONTRATADA. O horário de funcionamento do serviço é de 24 horas por dia, 7 dias por semana.

1.5. **PORTAL DE ITSM**

1.5.1. A CONTRATADA deverá fornecer acesso a uma plataforma ITSM. Deve ser um aplicativo baseado na web, disponível globalmente, que permita que a PREFEITURA interaja, gerencie e monitore seu serviço de segurança gerenciado.

1.6. **IDIOMAS SUPORTADOS**

1.6.1. O serviço deve ser entregue em inglês e português e as comunicações sistêmicas podem ser feitas em inglês ou em português.

1.7. **COMUNICAÇÕES**

1.7.1. **INFRAESTRUTURA DE SERVIÇO GERENCIADO DE SEGURANÇA**

1.7.1.1. A CONTRATADA deve utilizar uma infraestrutura com segurança integrada e por princípios de security by design. Deve ser altamente resiliente, segura e usar metodologias, ferramentas e técnicas de práticas recomendadas.

1.8. **NOTIFICAÇÕES**

1.8.1. Email

1.8.1.1. Por razões de segurança e privacidade de dados, as notificações por e-mail conterão apenas informações mínimas para notificar a PREFEITURA sobre a criação ou atualizações de tíquetes.

1.8.1.2. A PREFEITURA pode enviar e-mails relacionados a chamados novos ou existentes para a CONTRATADA. No caso em que nenhum número de referência for fornecido conforme formatado pela CONTRATADA, a CONTRATADA irá criar um chamado com uma breve descrição com base no assunto do e-mail enviado.

1.8.1.3. A PREFEITURA dará sempre preferência para abertura de chamados via portal ITSM da CONTRATADA.

1.8.2. Arquivos anexados

1.8.2.1. Diagramas, imagens, PDFs, executáveis e quaisquer outros anexos não devem ser anexados a nenhum caso por e-mail. Onde os anexos de arquivo deverão ser necessários, a PREFEITURA ou a CONTRATADA devem fazer login no portal da PREFEITURA e anexar o arquivo com segurança por meio de seu navegador conectado ao portal.

1.8.3. Telefone

1.8.3.1. A PREFEITURA poderá abrir chamados e entrar em contato com o Service Desk da CONTRATADA por telefone.

## 1.9. ENGENHARIA

1.9.1. Acesso ao item de configuração

1.9.1.1. O acesso de linha de comando aos consoles de gerenciamento dentro das instalações da PREFEITURA deve ser protegido por protocolos de acesso remoto com segurança e realizado através da VPN estabelecida.

1.9.2. Acesso a Aplicação

1.9.2.1. Os protocolos específicos de aplicativos para acessar consoles de gerenciamento dentro das instalações e ambientes da PREFEITURA deverão ser protegidos usando SSH v2 e HTTPS, aproveitando a VPN estabelecida. Os aplicativos SaaS de terceiros deverão ser acessados por meio da Internet pública, utilizando os protocolos de segurança escolhidos pelos fornecedores.

## 1.10. TRANSIÇÃO DO SERVIÇO

1.10.1. A transição do serviço deverá ser executada e planejada pela CONTRATADA, obedecendo as seguintes regras gerais:

1.10.1.1. Durante o período de transição do serviço, nenhum alerta, incidente ou caso deverá ser gerado para revisão e triagem.

1.10.1.2. A CONTRATADA deverá realizar, ao menos, uma reunião de Kick-off para comunicar o cronograma esperado de recursos e a execução do projeto, bem como confirmar que o escopo do trabalho é compreendido e as entregas deverão ser acordadas.

1.10.1.3. A CONTRATADA deve criar um cronograma conjunto do projeto após a reunião de kickoff, por meio de uma série de reuniões, descrevendo os prazos de entrega e marcos, usando um modelo detalhado de Cronograma de Gerenciamento do Projeto.

1.10.1.4. A CONTRATADA deve revisar toda a documentação relativa ao Serviço gerenciado de Segurança.

1.10.1.5. A CONTRATADA deve ser responsável por todas as implantações necessárias para o monitoramento a ser provido por seus serviços.

1.10.1.6. A CONTRATADA deverá ser responsável pelo onboarding dos equipamentos e soluções, ingestão de log (s), teste de serviço e verificação final

1.10.1.7. A CONTRATADA deverá ser responsável pela garantia de qualidade e ativação do (s) serviço (s)

1.10.1.8. A CONTRATADA deverá ser responsável pela validação final de conectividade com o Centro de operações de Segurança e as plataformas de segurança da PREFEITURA

1.10.1.9. A CONTRATADA deverá construir documentação de riscos e problemas

1.10.1.10. A CONTRATADA deverá realizar a reunião de sincronização de Serviço Gerenciado de Segurança da

CONTRATADA com a PREFEITURA

1.10.1.11. A CONTRATADA deverá realizar treinamento do portal do Serviço Gerenciado de Segurança para a equipe da PREFEITURA

1.10.1.12. A CONTRATADA deverá testar, revisar, documentar e avaliar o escopo de serviço e, junto com a PREFEITURA, estabelecer a data de início dos serviços após a configuração e ajustes necessários para prestação destes.

1.10.1.13. A CONTRATADA deverá ser responsável pela arquitetura da solução final.

1.10.1.14. A CONTRATADA deverá ser responsável pela conclusão e entregas. A equipe da CONTRATADA assume a operação. Isso envolve o monitoramento de alarmes gerados pelos dispositivos, execução dos ajustes, a manutenção e a garantia que o sistema esteja funcionando e alertando conforme o esperado.

## 1.11. GESTÃO DE SERVIÇOS

1.11.1. A CONTRATADA deverá prover um responsável pelos serviços do contrato, assim como a figura de um gestor de conta técnico, capaz de escalar prioridades e apoiar em momentos críticos ou de incidentes.

1.11.2. Também existira a função de um Gestor de contas técnico designado a PREFEITURA.

## 1.12. GESTOR DE ENTREGA DO CONTRATO

1.12.1. O gerenciamento de entrega de serviço deve fornecer governança e controle sobre os vários recursos de serviço, processos e sistemas necessários para gerenciar o ciclo de vida completo do serviço.

1.12.2. A CONTRATADA deverá designar um gestor de contrato na região contratante para ser responsável pelo gerenciamento do nível de serviço e agir como um intermediador da PREFEITURA para a CONTRATADA. Este colaborador da CONTRATADA é a interface principal que gerenciará o relacionamento de entrega de serviço entre sua organização e a PREFEITURA. O gestor é responsável por agendar, executar todas as reuniões de gerenciamento de serviço e garantir que todos os processos e documentação estejam em vigor para gerenciar seus serviços.

1.12.3. As entregas do gestor da CONTRATADA incluem:

1.12.3.1. Estabelecer relação com a PREFEITURA

1.12.3.2. Documentar atas, itens da agenda, ações e decisões

1.12.3.3. Gestão de mudanças

1.12.3.4. Gestão de problemas

1.12.3.5. Gerenciamento de escalonamento

1.12.3.6. Gerenciamento de riscos

1.12.3.7. Monitoramento, relatórios e gerenciamento de nível de serviço

1.12.3.8. Reunião de serviço

## 1.13. GERENTE DE CONTAS TÉCNICO

1.13.1. A CONTRATADA deverá disponibilizar um Gerente de Contas Técnico durante o contrato do Serviço Gerenciado.

1.13.2. O Gerente de contas técnico é uma função de gerenciamento de segurança que deve fornecer supervisão técnica baseada em riscos e serviços de defesa para a PREFEITURA. O serviço deve fornecer

profundidade e amplitude dos recursos da CONTRATADA de segurança cibernética.

1.13.3. Este gerente técnico deve utilizar as melhores práticas de segurança e uma ampla base de conhecimento para fornecer programas de segurança globalmente consistentes, adaptados às necessidades específicas da PREFEITURA e requisitos regulamentares. Deve estar empenhado em desenvolver relacionamentos de longo prazo com a equipe da PREFEITURA para obter um entendimento profundo de objetivos de negócios. Isso inclui a compreensão de suas iniciativas estratégicas, perfil de risco e avaliações do nível de maturidade da segurança cibernética. Este conhecimento e nível de envolvimento técnico garantem que a PREFEITURA se beneficiará de um serviço otimizado alinhado com as diretivas de negócios. Também devem se portar como os defensores da PREFEITURA perante a CONTRATADA, que identificam e rastreiam itens de ação e solicitações de serviço que foram criadas por meio do Service Desk da CONTRATADA para reduzir o tempo de resposta às solicitações. O gerente de conta técnico também deve fornecer uma função de controle de qualidade para garantir a excelência na entrega, manter altos níveis de satisfação, alcançar o sucesso do projeto e impulsionar a melhoria contínua do serviço.

## 1.14. SERVIÇO DE SEGURANÇA GERENCIADO

1.14.1. O escopo de Serviço de Segurança Gerenciado que a PREFEITURA deseja deve fornecer um serviço totalmente gerenciado 24 horas por dia, 7 dias por semana, incluindo integridade e disponibilidade e gerenciamento completo de mudanças. Ele também deve fornecer acordos de nível de serviço estendidos (SLAs) e objetivos, incluindo configuração e ajuste de dispositivo.

1.14.2. O serviço de Serviço de Segurança Gerenciado da CONTRATADA deverá seguir as melhores práticas da indústria para fornecer o cumprimento adequado e processos de gerenciamento de mudanças, eventos, incidentes e gerenciamento de problemas. Esses serviços garantem que os dispositivos de segurança estejam disponíveis e que a PREFEITURA mantenha a conformidade com os requisitos regulamentares aplicáveis.

## 1.15. RESUMO DOS SERVIÇOS ADQUIRIDOS

1.15.1. Acordo de nível dos Serviços adquiridos

| Serviço | Descrição | |
|---|---|---|
| **Serviços Gerenciados** | | |
| Serviços Gerenciados | ✓ | Operação 24x7, conforme matriz de serviços. |
| | Vigência | 48 meses |
| **Serviços Complementares** | | |
| Realização de mudanças, ajustes de configuração, remoção de itens, adição de configurações e acompanhamento | Vigência | 48 meses |

1.16. **MATRIZ DE SERVIÇOS**

1.16.1. A PREFEITURA busca serviços gerenciados de segurança. A CONTRATADA deve fornecer um conjunto central de módulos de serviço e elementos de serviço associados.

1.16.2. Matriz de Serviços desejada

| **Módulos e Elementos de Serviço** |
|---|
| Elementos de serviços principais |
| 24/7 Horas de Operação |
| Centros de Operações de Segurança |
| Portal Web para PREFEITURA |
| Suporte ao idioma |
| Gerenciamento de Dispositivos |
| Comunicações |
| Gestão de Escalonamento |
| Transição de Serviço |
| Recursos de gerenciamento de dispositivos |
| Saúde e Disponibilidade |
| Monitoramento de Saúde e Disponibilidade |
| Melhoria e Recomendação de Saúde e Disponibilidade |
| Implementação de mudanças de saúde e disponibilidade |
| Gerenciamento de Incidentes |
| Geração de Incidentes |
| Diagnóstico de Incidente |
| Resolução de Incidentes |
| Relatórios de Incidentes |

| Módulos e Elementos de Serviço |
|---|
| Gestão de Capacidades |
| Monitoramento e relatórios de capacidade |
| Recomendação de melhoria de capacidade |
| Planejamento de Capacidade |
| Implementação de mudança de capacidade |
| Rastreamento e relatórios de ativos |
| Controle de itens de configuração e atualizações |
| Relatório de status do item de configuração |
| Cumprimento de solicitação de serviço |
| Gerenciamento de solicitações de serviço |
| Gestão de Mudanças |
| Gerenciamento de Problemas |
| Identificação e Registro de Problemas |
| Relatórios de problemas |
| Identificação de Soluções |
| Implementação de soluções |

1.17. **REQUISITOS GERAIS**

1.17.1. Em todos os casos

1.17.1.1. O modelo de entrega padrão deve ser 24 horas por dia, 7 dias por semana, usando os SOCs da CONTRATADA.

1.17.2. Item de configuração

1.17.2.1. O serviço deverá gerenciar todos os itens de configuração suportados, definidos neste termo de referência.

1.17.3. Contatos de segurança designados

1.17.3.1. A PREFEITURA fornecerá dois membros da equipe para serem contatos de segurança e um contato de Service Desk para interagir com os serviços de gerenciamento de dispositivos.

1.18. **REQUISITOS DE COMUNICAÇÃO**

1.18.1. Acesso

1.18.1.1. Os serviços gerenciados de segurança exigem um acesso remoto seguro.

1.18.2. Conectividade – Serviços Gerenciados

1.18.2.1. A CONTRATADA deverá estabelecer conexão em modo VIRTUAL PRIVATE NETWORK com a PREFEITURA para poder monitorar e realizar acessos ao ambiente.

1.18.2.2. A PREFEITURA fornecerá, em tempo de transição, a lista de dispositivos a serem monitorados.

1.18.2.3. A PREFEITURA será responsável pela configuração SNMP nos equipamentos definidos na lista de dispositivos a serem monitorados, para obtenção de estatísticas.

1.18.2.4. A PREFEITURA será responsável por fornecer a topologia da rede para facilitar no entendimento do todo e na sugestão de alterações de desenho e melhorias.

1.19. **ELEMENTOS DE SERVIÇO PRINCIPAIS**

1.19.1. Horas de Operação

1.19.1.1. Os Serviços Gerenciados de Segurança deverão ser entregues através dos SOCs (Security Operations Centers, centros de operações de segurança) da CONTRATADA. A menos que seja declarado o contrário, as horas de operação deverão ser 24 horas por dia, 7 dias por semana.

1.19.2. Centros de Operação de Segurança

1.19.2.1. A CONTRATADA deverá prestar serviços através de Centro de Operação de Segurança próprio.

1.19.3. ITSM

1.19.3.1. A CONTRATADA deverá prover uma interface para ITSM, que é um aplicativo baseado na Web disponível globalmente, que permitirá que os usuários da PREFEITURA interajam, gerenciem e monitorem os Serviços gerenciados de segurança.

1.19.4. Suporte ao idioma

1.19.4.1. Os serviços deverão ser prestados em inglês e português do Brasil, a menos que haja acordo prévio e aprovação da PREFEITURA.

1.19.5. Gestão

1.19.5.1. O gerenciamento deverá ser fornecido como um componente central da oferta de serviços gerenciados de segurança, onde a PREFEITURA fornecerá a CONTRATADA um acesso privilegiado aos itens de configuração dentro do escopo.

1.19.5.2. A CONTRATADA deverá criar uma conta de administrador (Break Glass account) para a PREFEITURA e armazenará com segurança as credenciais e senha. No caso de uma emergência em que a CONTRATADA não consiga fazer uma alteração ou acessar a infraestrutura de configuração item/gerenciamento, o contato de segurança principal da PREFEITURA deverá ser fornecido com as credenciais e senha.

1.19.5.3. Cada vez que a PREFEITURA usar a conta Break Glass, a CONTRATADA deverá redefinir a conta com uma nova senha.

1.20. COMUNICAÇÕES

1.20.1. Infraestrutura do Serviço Gerenciado de Segurança

1.20.1.1. A CONTRATADA deverá utilizar uma infraestrutura regional com segurança incorporada por princípios de design. Deverá ser altamente resiliente e protegida e reconhecida pelo uso do melhor de metodologias, práticas, ferramentas e técnicas.

1.20.2. Notificações

1.20.2.1. Email

1.20.2.1.1. Por razões de segurança e privacidade de dados, as notificações por e-mail deverão conter apenas informações mínimas para notificar a PREFEITURA sobre a criação ou atualizações de casos. Esses e-mails não devem conter nenhuma informação sensível além do número de referência do ticket apropriado (e, quando possível, não divulgar qualquer informação privada na breve descrição do ticket).

1.20.2.1.2. A PREFEITURA poderá enviar e-mails relacionados a casos novos ou existentes para CONTRATADA. No caso de nenhum número de referência for fornecido, a CONTRATADA deverá criar um caso com uma descrição curta com base na linha de assunto fornecida.

1.20.2.2. Anexos de arquivos

1.20.2.2.1. Diagramas, imagens, PDF's, executáveis e quaisquer outros anexos não deverão ser anexados a nenhum caso por e-mail. Quando os anexos de arquivos forem necessários, a PREFEITURA fará através de seu navegador web conectado ao Portal.

1.20.2.3. Telefone

1.20.2.3.1. A equipe de segurança da CONTRATADA poderá entrar em contato com a PREFEITURA e a PREFEITURA pode entrar em contato com os Centros de Segurança da CONTRATADA por telefone. Em ambos os casos, uma autenticação deverá ser completada para verificar a identidade da PREFEITURA.

## 1.21. PORTAL ITSM DA CONTRATADA

1.21.1. Salvo declaração e acordo em contrário, todas as outras comunicações originárias dos SOCs deverão ser seguras, seguirão as melhores práticas de segurança e serão através do Portal Web da CONTRATADA.

1.21.2. Ferramenta ITSM (Service Management)

1.21.2.1. O módulo ITSM da CONTRATADA deverá gerenciar casos alinhados com a ITIL. Apenas a equipe CONTRATADA terá acesso à ferramenta ITSM.

1.21.3. Monitoração

1.21.3.1. Protocolos

1.21.3.1.1.1. Os itens de configuração da PREFEITURA devem ser monitorados utilizando vários protocolos, incluindo Simple Network Management Protocol (SNMP) v2, v3, Secure Shell (SSH) v2, Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) e Internet Control Message Protocol (ICMP).

## 1.22. EVENTOS DE MONITORAMENTO DE SAÚDE E DISPONIBILIDADE

1.22.1. Os feeds de eventos a partir de itens de configuração no escopo deverão ser enviados com segurança para o servidor de monitoramento através de uma VPN na infraestrutura do Serviço Gerenciado de Segurança.

## 1.23. ENGENHARIA

1.23.1. **Acesso ao item de configuração**

1.23.1.1. O acesso à linha de comando deverá ser protegido via SSH v2. Um jump-server da CONTRATADA confiável dentro da infraestrutura de Serviço Gerenciado de Segurança que aproveita a VPN (Virtual Private Network, rede privada virtual) deverá ser estabelecido para fornecer acesso SSH.

1.23.2. **Gestão de Escalonamento**

1.23.2.1. A CONTRATADA deverá fornecer um processo de escalonamento e definição de responsabilidades para abordar questões de escala. Para escalar um caso, a PREFEITURA poderá telefonar ou enviar um e-mail para o service desk (citando o número de referência).

1.23.2.2. A CONTRATADA poderá rebaixar um caso escalonado, se ele estiver sendo tratado dentro de um prazo ou resolução programada foi fornecida a PREFEITURA e em processo de teste. Para escalonamentos iniciados pela CONTRATADA, deverá ser obtido a aprovação da PREFEITURA antes de rebaixar um incidente de Segurança escalonado, solicitação de mudança ou solicitação de serviço.

1.23.2.3. Se for dada justificativa suficiente, a PREFEITURA poderá solicitar que seu caso seja escalonado para uma prioridade maior a qualquer momento. Após a reversão, o gerente do SOC deverá ser responsável por concordar com as ações.

1.23.3. **Transição de Serviço**

1.23.3.1. A transição do serviço deverá ser executada e planejada pela CONTRATADA, obedecendo as seguintes regras gerais:

1.23.3.2. Durante o período de transição do serviço, nenhum alerta, incidente, mudança ou caso deverá ser gerado para revisão e triagem.

1.23.3.3. A CONTRATADA deverá realizar, ao menos, uma reunião de Kick-off para comunicar o cronograma esperado de recursos e a execução do projeto, bem como confirmar que o escopo do trabalho é compreendido e as entregas deverão ser acordadas.

1.23.3.4. A CONTRATADA deve criar um cronograma conjunto do projeto após a reunião de kickoff, por meio de uma série de reuniões, descrevendo os prazos de entrega e marcos, usando um modelo detalhado de Cronograma de Gerenciamento do Projeto.

1.23.3.5. A CONTRATADA deve revisar toda a documentação relativa ao Serviço Gerenciado de Segurança.

1.23.3.6. A CONTRATADA deve ser responsável, em conjunto com a PREFEITURA, pelas implantações necessárias para o monitoramento, gerenciamento e operação a ser provido por seus serviços.

1.23.3.7. A CONTRATADA deverá verificar os acessos e contas disponibilizadas para gestão e administração.

1.23.3.8. A CONTRATADA deverá ser responsável pelas informações pertinentes para configuração de monitoramento de saúde e dos dispositivos a serem gerenciados.

1.23.3.9. A CONTRATADA deverá ser responsável pela garantia de qualidade e ativação do (s) serviço (s)

1.23.3.10. A CONTRATADA deverá ser responsável pela validação final de conectividade com o Serviço Gerenciado de Segurança

1.23.3.11. A CONTRATADA deverá construir documentação de riscos, problemas e procedimentos operacionais.

1.23.3.12. A CONTRATADA deverá realizar a reunião de sincronização entre o Serviço Gerenciado de Segurança de SOC com a PREFEITURA

1.23.3.13. A CONTRATADA deverá realizar treinamento do portal o Serviço Gerenciado de Segurança de SOC

com a PREFEITURA

1.23.3.14. A CONTRATADA deverá testar, revisar, documentar e avaliar o escopo de serviço do Serviço Gerenciado de Segurança, e, junto com a PREFEITURA, estabelecer a data de início dos serviços após a configuração e ajustes necessários para prestação destes.

1.23.3.15. A CONTRATADA deverá ser responsável pela arquitetura da solução final.

1.23.3.16. A CONTRATADA deverá ser responsável pela conclusão e entregas. A equipe da CONTRATADA assume a operação. Isso envolve o monitoramento de alarmes gerados pelos dispositivos gerenciados, sua operação, ajustes de regras e execução de solicitações efetuadas pela PREFEITURA para o escopo do Serviço Gerenciado de Segurança.

1.23.4. **Recursos de gerenciamento de dispositivos**

1.23.4.1. A PREFEITURA descreve abaixo as características do serviço gerenciado de segurança:

1.23.5. **Monitoramento de Saúde e Disponibilidade**

1.23.5.1. O serviço gerenciado de segurança deverá monitorar os principais indicadores de desempenho do estado de serviço e utilização de recursos do item de configuração no escopo para determinar a saúde, o desempenho e a disponibilidade em geral. O serviço deverá gerar automaticamente incidentes no sistema com base nos eventos, que excedem os limites em relação aos thresholds estabelecidos. O engenheiro do Serviço Gerenciado de Segurança da CONTRATADA deverá investigar e analisar os eventos para determinar uma possível ação corretiva ou de controle para resolver o incidente relacionado.

1.23.6. **Melhoria e Recomendação de Saúde e Disponibilidade**

1.23.6.1. A CONTRATADA deverá utilizar ciclos e limiares de pesquisa padrão ao monitorar itens de configuração no escopo. A CONTRATADA deverá ajustar os limiares com base nos dados históricos coletados para eliminar eventos desnecessários que ocorrem. Com esses dados, deverá identificar métodos potenciais para melhorar o desempenho do item de configuração e a saúde e a disponibilidade em geral.

1.23.6.2. A PREFEITURA também poderá solicitar a personalização de limites através de processos de gerenciamento de mudança padrão.

1.23.7. **Implementação de mudanças de saúde e disponibilidade**

1.23.7.1. Se um item de configuração exigir alterações, a CONTRATADA seguirá o processo padrão de gerenciamento de alterações descrito na seção Gerenciamento de Gestão de Mudanças.

1.24. **GERENCIAMENTO DE INCIDENTES**

1.24.1. O Gerenciamento de Incidentes se concentrará em responder a qualquer interrupção não planejada na operação de itens de serviço e configuração para minimizar qualquer impacto nas operações de negócios e garantir a qualidade e a disponibilidade do serviço.

1.24.2. **Geração de Incidentes**

1.24.2.1. Os incidentes podem ser gerados através do Monitoramento de Saúde e Disponibilidade pelo Serviço Gerenciado de Segurança ou PREFEITURA abrindo um caso de Incidente através do Portal ou chamada

telefônica para o Serviço Gerenciado de Segurança.

1.24.2.2. Após um caso de incidente ser criado através do Portal, com um Impacto e Urgência fornecidos, a equipe do Serviço Gerenciado de Segurança validará o ticket e modificará o Impacto e a Urgência, conforme necessário.

1.24.2.3. Para um caso de incidente levantado através de uma chamada telefônica para o SOC, o SOC deverá criar um caso de incidente em nome da PREFEITURA com o impacto e urgência relevantes.

1.24.2.4. **Diagnóstico de Incidente**

1.24.2.4.1. Os casos de incidente deverão ser gerenciados com base na prioridade do ticket de incidente levantado no Portal. As prioridades deverão ser calculadas com base no impacto e Urgência de um caso de incidente. As prioridades deverão ser definidas como Principal, Alta, Moderada e Baixa, conforme descrito na tabela abaixo:

1.24.2.4.2. **Matriz impacto-urgência de Serviços**

| | | **Urgência** | | |
|---|---|---|---|---|
| **Impacto** | | 1. Trabalho bloqueado | 2. Trabalho degradado | 3. Trabalho não afetado |
| | Toda a organização | Principal | Principal | Alto |
| | Vários departamentos | Principal | Alto | Moderado |
| | Departamento único | Alto | Moderado | Baixo |
| | Individual | Moderado | Baixo | Baixo |

1.24.2.4.2.1. A equipe do Serviço Gerenciado de Segurança deverá realizar a triagem do incidente para avaliar a prioridade. Incidentes deverão ser atribuídos ao engenheiro do Centro de Segurança apropriado para investigação e análise mais aprofundada para identificar um plano de correção para resolver o caso do incidente. Por meio do portal, a PREFEITURA deverá ser notificada de atualizações de um incidente e qualquer plano de restauração para resolver o caso.

1.24.2.5. **Gestão de Capacidades**

1.24.2.5.1. Monitoramento e relatórios de capacidade

1.24.2.5.1.1. Os sistemas de monitoramento utilizados no serviço de Gerenciamento de Dispositivos deverão verificar regularmente vários pontos de telemetria. Através do monitoramento contínuo, deverá ser possível destacar tendências potencialmente impactantes. Isso deverá ser utilizado para determinar se há um problema que precisa ser resolvido ou se os itens de configuração estão se tornando sobrecarregados

demais, por exemplo, um preenchimento de disco com dados de log. Usando isso como ponto de partida para gerenciamento de incidentes ou problemas, a CONTRATADA trabalhará com a PREFEITURA para aconselhar sobre resolução potencial ou mitigar o risco.

1.24.2.5.1.2. A CONTRATADA deverá utilizar limites padrão ao coletar dados de monitoramento. Reconhecemos que esses limites podem não ser aplicáveis a alguns ambientes da PREFEITURA, a CONTRATADA deverá trabalhar com a PREFEITURA para ajustar os limites durante o processo de Transição de Serviço ou após a entrada do serviço, onde uma linha de base poderá ser identificada.

1.24.2.5.2. Recomendação de melhoria de capacidade

1.24.2.5.2.1. Quando o monitoramento da CONTRATADA determinar que um dispositivo está sobrecarregado, deverá entrar em contato com a PREFEITURA para determinar o melhor plano e caminho a seguir. Exemplos incluem, mas não se limitam ao seguinte:

1.24.2.5.2.2. Solicitar a PREFEITURA que altere os níveis de registro ou a arquitetura de rede

1.24.2.5.2.3. Solicitar a PREFEITURA que altere os níveis de monitoramento dentro do item de configuração (por exemplo, desligar o registro de depuração)

1.24.2.5.2.4. Solicitar a PREFEITURA a atualização de hardware ou licenças para facilitar maior capacidade

1.25. **PLANEJAMENTO DE CAPACIDADE**

1.25.1. Com os dados de tendência acima mencionados disponíveis, CONTRATADA, Parceiros e/ou PREFEITURA poderão tomar decisões sobre requisitos futuros e crescimento esperado. Isso fornecerá um planejamento avançado inestimável para os responsáveis pelo orçamento ou planejamento de capacidade. Por exemplo, relatórios de análise de tendências mostrarão o consumo de disco ao longo do tempo, o que pode ser um indicador da necessidade de obter novos hardwares ou armazenamento adicional no próximo ciclo de orçamento.

1.25.2. **Implementação de mudança de capacidade**

1.25.2.1. Através da medição consistente e uniforme da telemetria a partir de itens de configuração de segurança gerenciados, a CONTRATADA deverá fazer recomendações ou levantar um ticket para mudança a ser aprovado pela PREFEITURA para melhorar ou evitar problemas futuros de capacidade que possam surgir. Isso é sujeito a aprovações necessárias e os conselhos que estão sendo seguidos. Quaisquer problemas de capacidade relacionados à atualização ou design de hardware não estão no escopo este serviço.

1.26. **RASTREAMENTO E RELATÓRIOS DE ATIVOS**

1.26.1. **Gravação de itens de configuração**

1.26.1.1. A CONTRATADA deverá registrar e rastrear itens de configuração da PREFEITURA no escopo com informações disponíveis no Portal.

1.26.2. **Controle de itens de configuração e atualizações**

1.26.2.1. **Hotfix e patches de segurança**

1.26.2.1.1. A CONTRATADA deverá monitorar o OEM (Original Equipment Manufacturer, fabricante de

equipamentos originais) em relação aos patches, hotfixes de segurança e atualizações de versão associadas aos itens de configuração no escopo. Também revisar tais lançamentos para aplicabilidade. Se determinar que tais atualizações ou patches deverão ser recomendados por razões de segurança ou operacionais, deverá solicitar aprovação antes de implementar qualquer atualização(s).

1.26.2.1.2. A CONTRATADA deverá instalar um número ilimitado de patches de software qualificados e aplicáveis e atualizações de versão menor do Sistema Operacional (OS) para os itens de configuração no escopo. Todos os patches ou upgrades de versão menores deverão ser considerados Alterações Normais, portanto, todos os processos aplicáveis de Gerenciamento de Alterações deverão ser aplicados.

1.26.2.1.3. Se a CONTRATADA determinar que o item de configuração no escopo da PREFEITURA é suscetível a uma nova vulnerabilidade, que é classificada como Baixa ou Média, deverá buscar a aprovação da PREFEITURA antes de tomar quaisquer medidas de resposta. Caso um engenheiro do SOC considere uma nova vulnerabilidade classificada como Alta em gravidade, a CONTRATADA deverá tomar medidas de resposta imediata através de um Caso de Mudança de Emergência.

1.26.2.2. **Principais atualizações de versão**

1.26.2.2.1. As principais atualizações de versão requerem planejamento cuidadoso, coordenação, gerenciamento e planejamento de reversão. A CONTRATADA deverá considerar todas as principais atualizações de versão como de alto risco no que diz respeito aos ambientes de produção da PREFEITURA e serão tratadas pontualmente.

1.26.2.2.2. A CONTRATADA deverá coordenar todas as principais atualizações de versão com a PREFEITURA e concordar em apresentar um projeto de preço fixo ou realizar o trabalho em uma base de tempo e materiais para execução destes serviços.

1.26.2.3. **Assinaturas**

1.26.2.3.1. **Atualizações de assinatura**

1.26.2.3.1.1. Sempre que aplicável, os bancos de dados de assinatura de itens de configuração que geralmente deverão ser automatizados e requerem conectividade entre o item de configuração e a Internet para baixar as atualizações, deverão ser verificados se as atualizações de assinaturas estão sendo atualizadas com sucesso.

1.26.2.3.2. **Falhas de assinatura**

1.26.2.3.2.1. Se a atualização de assinatura falhar, um incidente deverá ser levantado em nome da PREFEITURA. Posteriormente, quaisquer erros relacionados à capacidade de um item de configuração de atualizar as assinaturas deverão ser resolvidos usando o processo padrão de gerenciamento de incidentes da CONTRATADA.

1.26.2.3.3. **Escalonamentos de assinaturas**

1.26.2.3.3.1. Se a causa da incapacidade do item de configuração de atualizar assinaturas for um erro ou deficiência no banco de dados do fabricante, a CONTRATADA deverá escalar o problema para o fabricante em nome da PREFEITURA.

1.26.2.3.4. **Responsabilidades da PREFEITURA de Assinatura**

1.26.2.3.4.1. A PREFEITURA é responsável pela compatibilidade, teste de aceitação do usuário e testes funcionais dentro do ambiente de produção da PREFEITURA. A PREFEITURA garante que todos os itens de configuração estejam conectados à internet para permitir a entrega de atualizações automatizadas de assinatura do fabricante de itens de configuração, diretamente através de um proxy ou através de um sistema de gerenciamento dedicado, sempre que aplicável.

1.26.2.3.5. **Assinatura - Contrato de nível de serviço implícito**

1.26.2.3.5.1. Se a falha de um mecanismo de atualização de assinatura for diagnosticada como um incidente relacionado ao fabricante, o nível de serviço para resolver o incidente estará de acordo com o contrato de fornecedor de terceiros do fabricante.

1.26.2.3.6. **Backup de itens de configuração**

1.26.2.3.6.1. A PREFEITURA deverá manter um backup do sistema de itens de configuração e configuração no escopo em caso de falha.

1.26.2.3.6.2. Antes de implementar uma solicitação de alteração, a CONTRATADA deverá aplicar um backup de configuração, sob supervisão da PREFEITURA e utilizar para reverter para a última configuração conhecida, no caso de uma falha ou de uma solicitação da PREFEITURA.

1.26.2.3.6.3. A CONTRATADA deverá fazer backup das seguintes informações do item de configuração (quando aplicável):

26.2.3.6.3.1. Configuração do sistema (SO e configuração)

26.2.3.6.3.2. Regras de configuração

26.2.3.6.3.3. Configuração de assinatura

26.2.3.6.3.4. Arquivos de configuração

26.2.3.6.3.5. Cumprimento de solicitação de serviço

1.26.2.3.6.4. A CONTRATADA deve realizar o cumprimento do serviço, que se concentra na solicitação de informações, conselhos ou acesso.

1.27. **GERENCIAMENTO DE SOLICITAÇÕES DE SERVIÇO**

1.27.1. As solicitações de serviço deverão ser gerenciadas através do processo ITIL e deverão ser levantadas através de um caso no Portal. A CONTRATADA rastreará, monitorará e relatará a obtenção de várias métricas de desempenho importantes mensalmente.

1.27.2. **Solicitação de Informações**

1.27.2.1. A PREFEITURA poderá solicitar informações sobre o desempenho, configuração ou outros aspectos dos itens de configuração no escopo através do Portal. A CONTRATADA deverá fornecer as informações na Solicitação de Serviço.

1.27.3. **Relatórios de solicitação de serviço**

1.27.3.1. Todos os incidentes, solicitações de serviço ou problemas deverão ser registrados no sistema e reportados através do Portal.

1.27.4. **Gestão de Mudanças**

1.27.4.1. A pedido da PREFEITURA, a CONTRATADA deverá implementar uma solicitação de alteração para itens de configuração no escopo de acordo com uma tarefa associada a um catálogo ou tarefa não padrão.

1.27.5. **Solicitações de origem da PREFEITURA**

1.27.5.1. Os contatos da PREFEITURA válidos devem enviar uma solicitação para caso de mudança dentro do Portal.

1.27.6. **Solicitações de origem CONTRATADA**

1.27.6.1. CONTRATADA poderá enviar um pedido para caso de mudança quando uma mudança de controle correta é necessária para resolver um problema ou incidente.

1.27.7. **Relatórios de mudanças**

1.27.7.1. Deverão sempre utilizar o Portal para informar e acompanhar todas as alterações.

1.27.7.2. A parte que faz uma mudança precisa abrir um pedido aplicável de mudança no Portal antes da implementação para garantir a coordenação entre ambas as partes.

1.27.8. **Solicitação de Mudança**

1.27.8.1. Todos os pedidos de tipos de alteração deverão seguir o processo de Gerenciamento de Mudanças e requerem aprovação da CONTRATADA. As tarefas deverão ser derivadas por tecnologia, o que corresponde ao número de Unidades Service utilizadas por cada tarefa.

1.27.8.2. **A PREFEITURA emprega 3 (três) tipos de solicitação de mudança. Deverão ser elas:**

1.27.8.2.1. **Mudança Normal**

1.27.8.2.1.1. Alterações normais requerem aprovação (tanto de CONTRATADA quanta PREFEITURA, respectivamente) antes de serem implementadas. Nem a PREFEITURA nem a CONTRATADA estão autorizados a aplicar alterações em nome do outro sem o consentimento documentado de indivíduos autorizados (documentados dentro de um Grupo de Aprovação de mudanças no Portal) de ambas as partes através de um pedido de alteração no Portal.

1.27.8.2.2. **Mudança Padrão**

1.27.8.2.2.1. Quando um ticket de mudança padrão for criado através do Portal, a CONTRATADA é autorizada pela PREFEITURA a aplicar mudanças sem solicitar autorização. No entanto, o processo de aprovação interno da CONTRATADA ainda será válido.

1.27.8.2.3. **Mudanças de emergência**

1.27.8.2.3.1. Uma mudança de emergência é considerada um pedido de mudança que deve ser implementado o

mais rápido possível, por exemplo, para resolver um incidente ou para implementar um patch de segurança. A CONTRATADA trabalhará com a PREFEITURA durante o processo de Gerenciamento de Mudanças.

1.27.8.2.4. **Cancelando um pedido de mudança**

1.27.8.2.4.1. A PREFEITURA poderá cancelar uma solicitação até 2 horas antes de qualquer alteração programada estar comprometida com configuração do dispositivo.

1.27.8.2.4.2. Se a PREFEITURA quiser reverter uma mudança que já foi implementada, a PREFEITURA enviará uma nova solicitação de serviço para alteração através do Portal.

1.27.8.2.5. **Implementação de Mudanças**

1.27.8.2.5.1. A parte que faz a mudança deve concluir e documentar as seguintes tarefas associadas a cada alteração:

1.27.8.2.5.2. Fazer backup da configuração de execução atual antes de alterar.

1.27.8.2.5.3. Garantir que uma cópia de qualquer software e/ou firmware aplicável esteja prontamente acessível.

1.27.8.2.5.4. Garantir que um plano de reversão esteja documentado se há problemas com a mudança.

1.27.8.2.5.5. Atribuir um número de ticket interno (se aplicável) para acompanhar a mudança para fins de auditoria.

1.27.8.2.5.6. Implementar e testar a mudança (na medida do possível – a responsabilidade de teste também é compartilhada com a PREFEITURA) para confirmar se a mudança atendeu aos requerimentos conforme especificado pelo requisitante.

1.27.8.2.5.7. Criar um backup da nova configuração após a implementação da mudança.

1.27.8.2.5.8. Atualizar o ticket de solicitação de serviço da CONTRATADA indicando se a mudança foi bem-sucedida ou não.

1.27.8.2.5.9. É imperativo que cada mudança esteja totalmente documentada dentro do Portal para garantir que a CONTRATADA ou a PREFEITURA possam rapidamente solucionar problemas quando ocorrerem consequências negativas inesperadas.

**Acordo de Nível de Serviço do Serviço Gerenciado de Segurança (SLA´s) para a equipe compartilhada do Centro de Operação de Segurança da CONTRATADA.**

| Categoria | Descrição | Prioridade | SLA | Penalidades | Limite de penalidade | Horário do Serviço |
|---|---|---|---|---|---|---|
| **Solicitação de** | A CONTRATADA | P1 e P2 | 15 Mins | 1% da | Até 5% do valor | 24/7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **serviço** | atribuirá uma Solicitação de Serviço com prioridade _ _____ dentro de _____ minutos após o recebimento do tíquete no Service Desk da CONTRATADA | P3 & P4 | 4 Hrs | taxa de serviço mensal | total do contrato ao longo dos 12 meses. | |
| **Solicitação resolvida** | A CONTRATADA resolverá uma Solicitação de Serviço com prioridade _____ dentro de _____ após o recebimento do tíquete no Service Desk da CONTRATADA. | P1 | 2 dias corridos | 1% da taxa de serviço mensal | Até 5% do valor total do contrato ao longo dos 12 meses. | 24/7 |
| | | P2 & P3 | 5 dias corridos | | | |
| | | P4 | 10 dias corridos | | | |
| **Incident Management – Response** | A CONTRATADA atribuirá um tíquete de Incidente com prioridade _ dentro de _____ após o recebimento do tíquete no Service Desk da CONTRATADA. | P1 & P2 | 30 Min | 1% da taxa de serviço mensal | Até 5% do valor total do contrato ao longo dos 12 meses. | 24/7 |
| | | P3 & P4 | 60 Min | | | |
| **Incident Management – Resolve** | A CONTRATADA resolverá um incidente prioritário dentro de após o recebimento do tíquete na Equipe de Gerenciamento de Dispositivos da CONTRATADAS. | P1 | 8 Hrs | N/A | N/A | 24/7 |
| | | P2 | 16 Hrs | | | |
| | | P3&P4 | 48 Hrs | | | |
| **Emergency Change Response** | A CONTRATADA atribuirá um tíquete de Mudança de Emergência dentro de _____ minutos após o recebimento do tíquete no Service Desk da | N/A | 30 Min | N/A | N/A | 24/7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | CONTRATADA | | | | | |
| **Change Response** | A CONTRATADA atribuirá um tíquete de Mudança dentro de ____ minutos após o recebimento do tíquete no Service Desk da CONTRATADA | N/A | 60 Min | N/A | N/A | 24/7 |
| **Change Implementation – Complete** | A CONTRATADA completará as alterações antes do final da janela de alteração, conforme acordado mutuamente entre a PREFEITURA e a CONTRATADA. | N/A | 95% | N/A | N/A | 24/7 |
| **Resolve Notification (Service Level Objective) – Notify** | A CONTRATADA fornecerá uma notificação de resolução para cada tíquete de Incidente dentro de _____ minutos após a restauração do serviço. | N/A | 30 Min | N/A | N/A | 24/7 |
| **Elaboração de documentos de GMUD envolvendo os ativos de segurança da CONTRATADA;** | A CONTRATADA irá elaborar documentos de mudança que envolvam os ativos gerenciados por seu serviço de segurança gerenciado. | N/A | 2 dias corridos | | | 24/7 |
| **Planejamento e implantação de Novas ferramentas e/ou funcionalidades no ambiente de segurança da** | A CONTRATADA irá analisar, junto com a PREFEITURA, o planejamento e o esforço necessário para implantação ou adição de funcionalidades presentes nas ferramentas e no | N/A | 7 dias corridos | | | 24/7 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **CONTRATADA** | escopo de soluções descrito neste termo de referência. | | | | | |

1.28. **ENTREGAS**

1.28.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a PREFEITURA definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal de segurança da CONTRATADA, a saber:

| DENOMINAÇÃO | FORMA DE CÁLCULO | FILTRO | AGRUPADOR | DESCRIÇÃO |
|---|---|---|---|---|
| Quantitativo de requisições abertas | Soma de requisições abertas | Requisições abertas | Requisições | Número total de requisições abertas |
| Quantitativo de requisições por função | Soma de requisições abertas por função | Requisições por função | Requisições por função | Número total de requisições por função |
| Quantitativo de requisições concluídas | Soma de requisições concluídas | Requisições concluídas | Requisições concluídas | Número total de requisições concluídas |
| TOP 10 – Ativos configurados | Soma do número de configurações por ativo | Requisições por ativo | Ativo | TOP do número de requisições por ativo |
| TOP 10 – Requisições por origem | Soma do número de requisições por origem | Requisições por origem | Origem | TOP do número de requisições por origem |
| TOP 10 – Aplicações configuradas | Soma do número de aplicações configuradas | Requisições por Aplicações | Aplicações | TOP 10 requisições por aplicações |

1.28.2. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da PREFEITURA ou forma virtual, por meio de solução de videoconferência.

1.29. **EXCEÇÕES**

1.29.1. A PREFEITURA entende que quaisquer exceções que possam surgir devido ao desvio ou tentativa de contornar os processos descritos aqui podem resultar em uma configuração(s) instável e/ou não compatível.

1.30. **RESPONSABILIDADES da CONTRATADA**

1.30.1. Revisar o incidente, solicitações de serviço e qualquer documentação sobre as mudanças realizadas pela PREFEITURA e buscar esclarecimentos sempre que necessário.

1.31. **Análise de impacto de mudança**

1.31.1. Como parte do processo de projeto de mudança, a CONTRATADA deverá realizar uma análise de impacto de mudança de acordo com todos os pedidos de casos de mudança (pré e/ou pós-implementação). A análise é realizada antes da implementação de qualquer solicitação de caso de alteração, para garantir:

1.31.1.1. Hardware/software atende a todos os pré-requisitos

1.31.1.2. Existem backups da versão/configuração anterior

1.31.1.3. Qualquer alteração é consistente com as melhores práticas de segurança e não compromete a rede, o serviço ou da CONTRATADA ou da PREFEITURA

1.31.1.4. Qualquer alteração é relevante para o ambiente da PREFEITURA

1.31.1.5. Qualquer alteração pode ser implementada dentro do prazo solicitado

1.31.2. A CONTRATADA deverá considerar a Análise de Impacto de Alteração completa quando a PREFEITURA abordar todas as questões levantadas durante a análise (se aplicável), e o engenheiro reconhecer o recebimento de um ticket válido para mudança através do Portal.

1.32. **Gerenciamento de Problemas**

1.32.1. **Identificação e Registro de Problemas**

1.32.1.1. A CONTRATADA deverá seguir as melhores práticas da ITIL para identificação e registro de problemas. A identificação de problemas será realizada de várias maneiras e normalmente resultará em um caso de problema na ferramenta ITSM e no Portal. Normalmente, os problemas deverão ser derivados de uma série de fatores, tais como:

1.32.1.2. **Incidentes repetidos de mesma ou similaridade dentro de uma única localidade ou em várias localidades**

1.32.1.2.1. Problemas compostos causados por múltiplos incidentes de natureza diferente dentro de uma única localidade;

1.32.1.2.2. Notificação de problema do Fabricante;

1.32.1.2.3. Falta de patch oportuno do Fabricante para resolver uma vulnerabilidade de segurança;

1.32.1.2.4. Análise de tendências;

1.32.1.2.5. Relatórios de problemas;

1.32.1.2.6. Todos os problemas deverão ser registrados no sistema ITSM da CONTRATADA e reportados através do Portal;

1.32.1.2.7. Identificação e gravação de soluções.

1.32.1.3. **Implementação de soluções**

1.32.1.3.1. A PREFEITURA e a CONTRATADA discutirão e concordarão com a melhor ou mais adequada solução, com a PREFEITURA sendo responsável por implementar como uma mudança controlada ou uma série de mudanças em consonância com o seu processo de mudança padrão.

## 2. SERVIÇO DE RESPOSTA A INCIDENTES CIBERNÉTICOS

2.1. A CONTRATADA deverá prover, dentro dos serviços de Serviço Gerenciados de Segurança, serviço adicional de resposta a incidentes identificados e reportados. Abaixo, são especificados o escopo de serviços requeridos pela PREFEITURA, a saber:

2.2. Atendimento 24x7x365 para responder a incidentes.

2.3. Manipulação de conformidade com evidências.

2.4. Implementação de ferramentas de Resposta a Incidentes.

2.5. Deve haver integração com o Serviço Gerenciados de Segurança da CONTRATADA para valor agregado.

2.6. Deve realizar análise forense digital especializada.

2.7. A CONTRATADA deve possuir equipe dedicada de engenharia reversa de malware.

2.8. A equipe da CONTRATADA altamente colaborativa com as equipes da PREFEITURA.

2.9. Análise de incidentes de segurança da informação.

2.10. Triagem de incidentes de segurança da informação (priorização e categorização).

2.11. Coleta de informações.

2.12. Coordenação detalhada da análise realizada.

2.13. Análise da causa raiz de incidentes de segurança da informação.

2.14. Análise de artefatos e evidências forenses.

2.15. Análise de mídia ou superfície.

2.16. Engenharia reversa.

2.17. Tempo de execução e/ou análise dinâmica.

2.17.1.1. Análise comparativa.

2.17.2. Mitigação e recuperação.

2.17.2.1. Estabelecer plano de resposta (Requer aprovação da PREFEITURA).

2.17.2.2. Medidas ad hoc e contenção.

2.17.2.3. Restauração de sistemas (Através do serviço de Gerenciamento de Dispositivos de Segurança).

2.17.2.4. Suporte de outras entidades de Segurança da Informação.

2.17.3. Coordenação de incidentes de segurança da informação.

2.17.3.1. Comunicação Interna.

2.17.3.2. Distribuição de notificação interna.

2.17.3.3. Distribuição interna de informações relevantes.

2.17.3.4. Coordenação de atividades.

2.17.3.5. Relatórios Internos.

2.17.4. Apoio à gestão de crises.

2.17.4.1. Distribuição de informações às partes interessadas e necessárias.

2.17.4.2. Relatório de status de segurança da informação.

2.17.4.3. Comunicação de decisões estratégicas.

2.17.5. Para todos os Serviços de Resposta a Incidente realizados, a CONTRATADA deverá elaborar e entregar um Relatório de Resposta a Incidentes com, no mínimo:

2.17.5.1. Sumário executivo.

2.17.5.2. Consultores designados para a investigação.

2.17.5.3. Análise do cronograma.

2.17.5.4. Resultados detalhados em todas as evidências analisadas.

2.17.5.5. Fornecimento de recomendações conforme identificações realizadas.

2.17.5.6. Caso necessário, o relatório também poderá ser apresentado aos Stakeholders em forma de apresentação (.ppsx e/ou .pdf).

2.17.6. O Teste de Plano de Resposta a Incidente de Segurança deverá atender os requisitos mínimos, a saber:

2.17.6.1. A CONTRATADA deverá realizar dois tipos de exercício de simulação: Resposta a Incidentes Técnicos e Gerenciamento de Crises Executivo. De acordo com as melhores práticas, cada tipo deverá ser conduzido anualmente, separadamente ou de forma integrada.

2.17.7. Para Resposta a Incidentes Técnicos, os cenários mais comuns avaliados nesses tipos de simulações são ataques que utilizam os vetores:

2.17.7.1. E-mails de Phishing.

2.17.7.2. Anexos maliciosos.

2.17.7.3. Requisições suspeitas.

2.17.7.4. Dispositivos não autorizados.

2.17.8. Para o Gerenciamento de Crises Executivo, os cenários e situações mais comuns abordando tópicos como:

2.17.8.1. Quando pagar extorsão ou ameaças de ransomware.

2.17.8.2. Tomada de decisão sobre o impacto de táticas de contenção.

2.17.8.3. Requisitos de divulgação de violações para reguladores e principais partes interessadas.

2.17.8.4. Melhores práticas de notificação da PREFEITURA.

2.17.8.5. Melhores práticas de comunicação pela mídia.

2.17.9. Para todo Teste de Plano de Resposta a Incidente de Segurança realizado, a CONTRATADA deverá entregar, no mínimo, as seguintes documentações:

2.17.9.1. Apresentação mostrando o resultado da simulação contendo interação dos participantes, lições aprendidas e recomendações estratégicas.

2.17.9.2. Relatório descrevendo a cronologia dos eventos, respostas dos participantes e as avaliações e recomendações para aperfeiçoamento.

2.17.9.3. Um roadmap mostrando os projetos recomendados a serem implementados baseados nas lições aprendidas e recomendações.

2.17.9.4. Deverá ser realizada uma apresentação dos principais pontos via ferramenta de reuniões on-line, no dia e horário acordados entre a PREFEITURA e a CONTRATADA.

2.17.9.5. **Serviço de Operação e Atendimento a Requisições**

2.17.10. Tem como objetivo gerir, manter e operar todos os serviços, soluções e produtos eventualmente fornecidos pela CONTRATADA para tal finalidade, realizando a interface com a PREFEITURA e a orquestração entre os demais serviços que são escopo desta contratação;

2.17.11. A CONTRATADA deverá disponibilizar no mínimo 01 profissional Certified Information Systems Security Professional (CISSP) que atuará em conjunto com o Gestor do Centro de Operações de Segurança, para servirem de contatos formais entre a CONTRATADA e a PREFEITURA.

2.17.12. A CONTRATADA deverá manter disponível em dias úteis em horário comercial (período das 09:00 às 17:00 horas) 01 (um) profissional com Certificação CISSP, pronto para ser acionado/demandado de forma imediata conforme necessidade da PREFEITURA, de forma presencial nas dependências da PREFEITURA ou de forma remota no Centro de Operações de Segurança da CONTRATADA. Em situações excepcionais, o profissional CISSP poderá ser acionado fora dos horários previstos nesta janela, para atuar e/ou auxiliar a equipe técnica da CONTRANTE na resolução de incidentes de segurança cibernética.

2.17.12.1.1. **Priorização de Chamados**

17.12.1.1.1. Caso hajam incidentes detectados pelo Centro de Operações de Segurança, a CONTRATADA vai atribuir a prioridade do incidente, seguindo frameworks e boas práticas de serviços gerenciados de segurança. Durante a fase de transição, essas definições serão avaliadas com a PREFEITURA e casos de uso específicos podem ser priorizados de acordo com o alinhamento.

17.12.1.1.2. A tabela abaixo explica os quatro níveis de prioridade disponíveis.

| Prioridade | Severidade | Exceção | Ações da CONTRATADA | Caso de uso |
|---|---|---|---|---|
| P1 | Risco Crítico Crítico | Caso de uso personalizado considerado pelo cliente como "crítico" | Análise, Validação e Alerta do Centro de Operações de Segurança | Malware detectado, mas não bloqueado em vários hosts |
| P2 | Alto Risco Alto | Todos os outros casos de uso personalizados que exigem análise Centro de Operações de Segurança | Análise, Validação e Alerta Centro de Operações de Segurança | Malware detectado, mas não bloqueado em um único host |
| P3 | Risco Mínimo /Histórico/Auditoria/Caso de Uso Personalizado | N/A | Relatório, Painel, retenção para conformidade | Malware detectado e bloqueado em vários hosts |

| | | | | |
|---|---|---|---|---|
| P4 | Baixo risco /Histórico/ Auditoria/Caso de uso personalizado | N/A | Relatório, Painel, retenção para conformidade | Malware detectado e bloqueado em um único host |

2.17.12.2. **Resolução de Incidentes**

2.17.12.2.1. A CONTRATADA deverá trabalhar para resolver os incidentes e movê-los para um estado resolvido no Portal de para permitir que a PREFEITURA confirme a resolução. Relatórios de Incidentes

2.17.12.2.2. A PREFEITURA deverá ser notificada de todos os incidentes por meio de um e-mail de notificação, que conterá informações mínimas para fins de segurança, com os detalhes completos do incidente disponíveis apenas através do Portal.

2.17.12.3. **Acordo de Nível de Serviço para o CSIRT (SLA´s)**

| Serviço | Sub-elemento de Serviço | Ação | Prioridade/ Frequência | Intervalo de Medição | Critério de Aceitação | SLA |
|---|---|---|---|---|---|---|
| CSIRT | Atribuição de Incidente | Atribuir | Todas | Mensal | 95% | 30 minutos |
| | Resolução de Incidente | Criação e iniciação do Plano de Resposta a Incidente | P1 | Mensal | 95% | 4 horas |
| | Resolução de Incidente | Criação e iniciação do Plano de Resposta a Incidente | P2 & P3 | Mensal | 95% | 8 horas |
| | Resolução de Incidente | Criação e iniciação do Plano de Resposta a Incidente | P4 | Mensal | 95% | 24 horas |

2.17.12.4. A PREFEITURA entende que um Banco de Horas de até 480 (quatrocentos e oitenta) horas ao longo dos 48 meses sob demanda, com o consumo estimado pela Prefeitura de 120 (cento e vinte) horas anuais utilizados como serviço de resposta a incidentes.

2.18. **GESTÃO DE SERVIÇOS**

2.18.1. A CONTRATADA deverá prover um responsável pelos serviços do contrato, assim como a figura de um gestor de conta técnico, capaz de escalar prioridades e apoiar em momentos críticos ou de incidentes.

## 3. SERVIÇOS TÉCNICOS CONTINUADOS DE SOLUÇÕES CISCO

### 3.1. AVALIAÇÃO E RECOMENDAÇÕES DE MELHORIAS NA REDE CISCO

3.1.1. O Serviço de Avaliação de Rede avalia a situação atual dos equipamentos de rede e serviços independentemente dos fabricantes envolvidos na solução de rede. O serviço deve focar nas questões de planejamento, otimização dos equipamentos e entrega de serviços no ambiente Cisco de modo a proporcionar a PREFEITURA o máximo de confiabilidade, segurança, disponibilidade e escalabilidade. O serviço inclui um relatório de assessement detalhado que inclui configuração da rede e equipamentos (lógica e física) bem como práticas e políticas existentes recomendando um plano de ação alinhado às necessidades do negócio.

3.1.2. A PREFEITURA espera que os seguintes serviços sejam entregues pela CONTRATADA:

3.1.2.1. Realizar o entendimento da situação atual a respeito da rede e serviços;

3.1.2.2. Realizar o troubleshooting de acordo com as melhores práticas do Fabricante Cisco para melhorar a disponibilidade e desempenho da rede;

3.1.2.3. Referendar a implementação de um processo de melhoria contínua;

3.1.2.4. Relacionar dados e informações atualizadas para o gerenciamento da configuração;

3.1.2.5. Fornecer recomendações para reduzir o tempo e riscos de implementação de novos serviços;

3.1.2.6. Aumentar a performance, capacidade e disponibilidade da rede;

3.1.2.7. Prestar suporte a PREFEITURA na decisão dos investimentos em equipamentos e soluções de rede.

3.1.3. Elaborar e atualizar documentações e procedimentos necessários para administração, operação e suporte do ambiente gerenciado, garantindo sua atualização sempre que necessário.

### 3.2. TROUBLESHOOTING E SERVIÇOS TÉCNICOS CONTINUADOS NOS EQUIPAMENTOS CISCO

3.2.1. A CONTRATADA deverá executar trabalho consultivo com o objetivo de manter a estabilidade e realizar ações proativas para maximizar o uso dos componentes da soluções Cisco, de modo a manter o ambiente disponível e íntegro.

3.2.2. Os serviços deverão ser executados em regime de horário 8x5, ou seja, 8 (oito) horas por 5 (cinco) dias úteis durante a semana.

3.2.3. A PREFEITURA espera que a CONTRATADA disponibilize Profissionais Técnicos compartilhados de Nível Expert em Redes e Segurança Cisco e Pleno de Wireless Cisco, alinhados a mesma duração do Apoio Técnico local também disponibilizado à PREFEITURA, para as ações necessárias e devida mitigação dos problemas técnicos, para levar trazer maior estabilidade da operação dos ativos Cisco da PREFEITURA.

3.2.4. O serviço de Grupo Técnico alocado na PREFEITURA atuará em conjunto com o Profissionais técnicos compartilhados da CONTRATADA para alinhar as ações e atividades de planejamento e troubleshooting, para maior celeridade na mitigação das questões encontradas.

3.2.5. A PREFEITURA espera da CONTRATADA o fornecimento de no mínimo 500 (quinhentas) horas por Consultor Sênior de Redes, além Profissional de Redes Cisco Expert em Redes (com certificação válida de CCIE Routing & Switching) e Consultor Sênior de Redes WIFI Cisco (com certificação CCNP Wireless válida), para o trabalho consultivo previsto no itens durante o período de 15 (quinze) meses.

3.2.6. A PREFEITURA espera ainda que a CONTRATADA disponibilize um um Gestor de Contrato de

Serviço compartilhado para servir de ponto focal entre a Equipe da PREFEITURA e a CONTRATADA.

3.2.7. A PREFEITURA espera que a contratação deste profissional para atuação local em suas instalações ocorra em até 90 (noventa) dias corridos, sem que ocorra glosas à CONTRATADA.

3.2.8. A CONTRATADA deve disponibilizar serviço compartilhado de Consultores de Segurança e Redes Experts Cisco compartilhados para apoiar nas atividades do Profissional Sênior de Redes Cisco, coordenando as ações de mitigação de problemas de conectividade e trazer maior estabilidade na operação dos ativos Cisco da PREFEITURA.

3.2.9. Devido a necessidades de atuar na melhoria dos controles de segurança ou executar atividades de intervenção em janelas específicas de horários e/ou dia, a PREFEITURA poderá demandar que o Profissional da CONTRATADA atue fora do horário estipulado acima, em cronograma devidamente estipulado.

3.2.10. A CONTRATADA deverá disponibilizar ainda um Gestor de Contrato de Serviço compartilhado, que será o ponto focal de contato perante a CONTRATADA, para quaisquer demandas pertinentes a Gestão dos profissionais dedicados e do trabalho Consultivo.

3.2.11. Atividades administrativas e de recursos humanos de responsabilidade da contratada não poderão ser executadas pelos colaboradores vinculados a um perfil profissional. Deve ser alocado recurso para tratar de assuntos rotineiros de ordem administrativa, de controle de contrato e faturamento. Este recurso não poderá ter suas horas cobradas.

3.2.12. A CONTRATADA deverá responsabilizar-se por eventuais danos, extravios ou desaparecimento decorrentes de ação (de maneira imperita, imprudente ou negligente) ou omissão de seus profissionais sobre quaisquer equipamentos, materiais, instalações e demais bens da PREFEITURA. Nestes casos, demonstrada a responsabilidade, a CONTRATADA deverá ressarcir o erário num prazo máximo de 60 (sessenta) dias, sob pena de retenção do valor equivalente ao dano no próximo pagamento.

3.3. **OBSERVAÇÕES:**

3.3.1. A PREFEITURA espera que a CONTRATADA disponibilize Profissionais de Nível Expert em Redes e Segurança Cisco e Profissional Nível Sênior Wireless Cisco durante o contrato, para apoio do Profissional onsite disponibilizado pela CONTRATADA à PREFEITURA, para o desenvolvimento dos Serviços previstos neste Termo.

3.3.2. Os serviços deverão ser executados em regime de horário 8x5, ou seja, 8 (oito) horas por 5 (cinco) dias úteis durante a semana.

3.4. **AVALIAÇÃO E RECOMENDAÇÕES DE SEGURANÇA DA INFORMAÇÃO**

3.4.1. A CONTRATADA deverá realizar, através de serviços de avaliação de segurança, ajustes e recomendações relacionados aos processos e padrões especificados pela PREFEITURA .

3.4.2. Como parte de qualquer organização que possui iniciativas de melhoria da segurança da informação, é sempre recomendável, e na maioria dos casos, rever o estado atual da arquitetura de segurança e compreender a necessidade de melhoria necessária para permitir que a organização elabore um plano de ação que garanta a adequação continuada da gestão de riscos, além de manter a conformidade com regulamentações externas e mandatos contratuais.

3.4.3. Para atingir estes objetivos, a CONTRATADA desenvolverá um processo de avaliação para ajudar a PREFEITURA a avaliar de forma global os processos e a arquitetura da segurança da informação da sua empresa e identificar áreas específicas que precisam ser melhoradas. Baseado em melhores práticas de mercado, e na experiência prática e conhecimento da indústria de tecnologia, esta avaliação de segurança da informação deverá fornecer a educação e orientação necessária para entender e começar a aplicar ações de governança corporativa de segurança.

3.4.4. O principal objetivo das horas de consultoria será acelerar e apoiar a PREFEITURA na adoção dos serviços gerenciados de segurança e aumenta o nível de maturidade de Segurança da Informação e cibersegurança.

3.4.5. Deverá ser estabelecida em conjunto, CONTRATADA e PREFEITURA , as prioridades dos serviços de consultoria, assim que definido o plano de trabalho as atividades consultivas de cibersegurança poderão ser realizadas.

3.4.6. As horas contratadas para consultoria devem ser consumidas através das seguintes atividades, exclusivamente:

3.4.6.1. Identificação, desenvolvimento, implementação e manutenção de processos corporativos

3.4.6.2. Avaliação Periódica do plano de resposta a incidentes

3.4.6.3. Apoio para construção/readequação na arquitetura de segurança

3.4.6.4. Condução de GAP Analysis de Segurança e frameworks específicos

3.4.6.5. Identificação de oportunidades para melhorias no ambiente (Estratégias, Serviços, Plataformas)

3.4.6.6. Análise de Riscos de Segurança

3.4.6.7. Políticas e Procedimentos

3.4.6.8. Treinamento de conscientização dos usuários em segurança cibernética

3.4.7. **IDENTIFICAÇÃO, DESENVOLVIMENTO, IMPLEMENTAÇÃO E MANUTENÇÃO DOS PROCESSOS CORPORATIVOS**]

3.4.7.1. A CONTRATADA deverá utilizar-se de frameworks como o NIST Cyber Security Framework, CIS Controls, ISA/IEC 62443, juntamente com os padrões de segurança da série ISO/IEC 27000, como uma base para transmitir as pessoas adequadas, processos e tecnologia necessários para suportar o ciclo de vida da segurança dentro da PREFEITURA e auxiliar na manutenção dos processos corporativos com foco em segurança.

3.4.8. **APOIO PARA CONSTRUÇÃO/READEQUAÇÃO NA ARQUITETURA DE SEGURANÇA**

3.4.8.1.1. Consultoria para apoio na Arquitetura de Segurança Lógica e Modelo de Domínio de Segurança com a Estrutura de Classificação de Segurança da Informação com abordagem em camadas de defesa profunda, baseada em:

3.4.8.1.2. Conjunto de controles para a classificação de domínio

3.4.8.1.3. Nível de isolamento por domínio

3.4.8.1.4. Controles técnicos e não técnicos nos níveis de Operações, Aplicações, Terminais e Infraestrutura

3.4.9. **CONDUÇÃO DE ANÁLISE DE GAP DE SEGURANÇA E FRAMEWORKS ESPECÍFICOS**

3.4.9.1. **IDENTIFICAÇÃO DE OPORTUNIDADES PARA MELHORIAS NO AMBIENTE (ESTRATÉGIAS, SERVIÇOS, PLATAFORMAS)**

3.4.9.1.1. Apoio de consultoria para recomendações de novas soluções, serviços e adequações na operação conforme evolução da área de segurança.

3.4.9.1.2. Elaborar e atualizar documentações e procedimentos necessários para administração, operação e suporte do ambiente gerenciado, garantindo sua atualização sempre que necessário.

3.4.9.2. **ANÁLISE DOS RISCOS DE SEGURANÇA**

3.4.9.2.1. Realização de Risk Analysis associado a vulnerabilidades encontradas em ambientes de IT (Análise de Vulnerabilidades Tecnológicas) e com os resultados da Análise de Conformidade.

3.4.9.2.2. A metodologia e framework utilizado para o serviço de Análise de Riscos em Segurança deve ser a ISO/IEC 27005.

3.4.9.2.3. Sua abordagem e metodologia devem ser usadas em combinação com outros padrões de segurança de TI, como a série ISO 27000 que tem o foco em:

3.4.9.2.3.1. Confidencialidade (C), Integridade (I), Disponibilidade (A)

3.4.9.2.3.2. Sistema de gerenciamento de segurança da informação (SGSI)

3.4.9.2.3.3. Classificação de informações, análise de riscos, conceito de segurança

3.4.9.2.3.4. Abordagem Plan-Do-Check-Act para segurança de TI

3.4.9.2.3.5. Entregáveis:

.4.9.2.3.5.1. Relatório Executivo (Riscos mapeados, Controles encontrados, Recomendações, Riscos Residuais)

.4.9.2.3.5.2. Planilha Técnica (Matriz de Riscos, Vulnerabilidades, Impacto, Ameaças, Ativos, Controles, Ricos Atuais X Riscos Residuais, Probabilidade)

3.4.10. **ESCOPO DA AVALIAÇÃO DE ESTADO DE MATURIDADE DO BACKUP**

3.4.10.1. A PREFEITURA espera que os consultores de segurança entendam as práticas atuais de segurança da informação da PREFEITURA e as relacionem com uma estrutura de backup resiliente alinhada a continuidade do negócio, assim identificando possíveis lacunas ("gaps"), além de apontar recomendações e soluções necessárias e desenvolver um roadmap/cronograma para as devidas correções.

3.4.10.2. Isso envolverá consultar as partes interessadas para garantir que haja rastreabilidade desde os objetivos de negócios, riscos e requisitos de conformidade até as políticas reais aplicadas pelos controles de segurança.

3.4.10.3. A CONTRATADA deve fazer uso de metodologia e estrutura de arquitetura de segurança para garantir que haja rastreabilidade completa dos objetivos de negócio da PREFEITURA, sendo riscos de negócios, requisitos de segurança. Para tanto, as atividades devem estar em conformidade ao Framework CMMI (Capability Maturity Model Integration), que garante visibilidade do grau de maturidade em que uma organização se encontra, classificados em:

3.4.10.3.1. Nível 0 - Inexistente: Sem existência de processos ou Ferramentas relacionadas;

3.4.10.3.2. Nível 1 - Inicial: Imprevisível e reativo. O trabalho é executado, mas muitas vezes está atrasado ou acima do orçamento. Sem ferramentas adequadas, mas em fase de planejamento;

3.4.10.3.3. Nível 2 - Repetitivo: Gerenciado no nível de projeto. Os projetos são planejados, executados, medidos

e controlados e já existem ferramentas adequadas, porém com funcionalidades básicas habilitadas;

3.4.10.3.4. Nível 3 - Definido: Proativo ao invés de reativo. Os padrões de toda a organização fornecem orientação em projetos, programas e portifólio. Automações são realizadas nos níveis de ferramenta ou integrações com soluções terceiras;

3.4.10.3.5. Nível 4 - Gerenciado: Medido e controlado. A organização é orientada por dados com objetivos quantitativos para melhoria de desempenho e revisadas ao menos anualmente. Os relatórios emitidos pelos sistemas avaliados são constantemente verificados e comparados com dados anteriores e/ou baseline;

3.4.10.3.6. Nível 5 - Otimizado: Estável e Flexivel. A organização está focada na melhoria continua e está constituída de forma a responder a oportunidades e mudanças. Existe o conhecimento, engajamento e consentimento da alta gestão na perspectiva dos processos avaliados. As ferramentas avaliadas são configuradas para um nível de automação completo, que inclua inteligência suficiente para a otimização de processos manuais ou acionamentos entre áreas distintas.

3.4.10.4. A avaliação do grau de maturidade deve ser dividida em 3 pilares principais:

3.4.10.4.1. Arquitetura de Backup: deve ser abordada a maturidade a respeito da arquitetura de backup, levando em consideração conceitos como retenção dos dados, distribuição das cópias e funcionalidades existentes x usadas na ferramenta de backup.

3.4.10.4.2. Arquitetura Cyber Resiliente: deverá ser demonstrada a maturidade a respeito da arquitetura de backup que ofereça funções adicionais de detecção/recuperação/proteção, levando em consideração conceitos como air gap, imutabilidade, avaliação pós-infecção e funcionalidades de segurança avançadas.

3.4.10.4.3. Planejamento e Processo: Deve ser aboardada a maturidade a respeito do planejamento e dos processos envolvidos quanto à backup e restore, levando em consideração requisitos como PRD (Plano de Recuperação de Desastres), políticas de backup, definições de priorização de aplicações, execução de testes e definições de RPO (Recovery Point Objective) e RTO (Recovery Time Objective).

3.4.10.5. A CONTRATADA deverá entregar workshops técnicos e não técnicos, revisões de documentação e exercícios de arquitetura, bem como um conjunto de Avaliações Técnicas e Testes definidos, conforme definido pelo escopo. Todo o processo de avaliação será embasado em frameworks de boas práticas da indústria como NIST CSF, ISO/IEC 27001, ISO/IEC 27005 e CIS Controls.

3.4.10.6. A CONTRATADA deverá realizar avaliações juntamente com as partes interessadas (stakeholders) da PREFEITURA, a fim de fornecer orientações para garantir que os resultados adequados sejam atendidos.

3.4.10.7. **ABORDAGEM**

3.4.10.8. A CONTRATADA deverá utilizar abordagem TOP-DOWN para a segurança da informação, buscando total alinhamento com o negócio da PREFEITURA, para proporcionar rastreabilidade e justificativa para os controles de segurança, técnicos e não técnicos. Todas as práticas de segurança da informação e gestão de risco devem ser práticas, apropriadas e economicamente proporcionais para garantir que esforços e recursos sejam utilizados de forma consciente e sustentável.

3.4.10.9. **METODOLOGIA APLICADA**

3.4.10.10. A PREFEITURA espera que a equipe da CONTRATADA faça o devido engajamento das equipes e áreas interessadas da PREFEITURA:

3.4.10.10.1. Para entenderem a atual situação da maturidade backup;

3.4.10.10.2. Apoiar na definição da solução ou conjunto de soluções mais eficazes;

3.4.10.10.3. Identificar áreas prioritárias para ação.

3.4.10.11. Caso a PREFEITURA desejar, poderá adquirir pacote adicional de horas para permitir que a CONTRATADA realize além do apoio estratégico, apoie também na implementação e gestão da(s) solução(ões).

3.4.10.12. **ENTREGÁVEIS E CRONOGRAMA DE ATIVIDADES**

3.4.10.13. A CONTRATADA deve apresentar os detalhes do escopo do serviço, aonde serão especificadas as documentações, processos e definições que devem ser realizadas do ponto de vista de pessoas e processos, alinhados a visão estratégica da PREFEITURA. A CONTRATADA deverá entregar os seguintes Entregáveis à PREFEITURA:

| # | ATIVIDADE | DESCRIÇÃO |
|---|---|---|
| 1 | Análise de Documentos e Políticas | Análise da Política, Padrões e Procedimentos relacionados ao Backup e ao Plano de Recuperação de Desastres |
| 2 | Planejamento de Atividades e Assessment | Organização, criação de cronograma, planejamento de atividades, definição das áreas entrevistadas e alinhamentos pré-assessment. |
| 3 | Entrevistas com áreas de negócio | O diagnóstico será feito envolvendo as áreas selecionadas da PREFEITURA. As entrevistas serão realizadas com colaboradores previamente definidos. |
| 4 | Entrevistas com áreas de TI | Entrevista com áreas pré-selecionadas e escolhidas conforme necessidade. |
| 5 | Consolidação de Resultados | Análise das informações providas pela PREFEITURA, de forma identificar os gaps, forças e fraquezas de processos, tecnologias e pessoas, aumentar a visibilidade da maturidade atual do ambiente e arquitetura de backup. |
| 6 | Confecção de Relatório | Elaboração de relatório com base nas entrevistas realizadas com visibilidade sobre processos, tecnologias e pessoas que compõem toda a visão estratégica de segurança da empresa. |
| 7 | Construção de Roadmap | Roadmap de evolução para mitigar os gaps encontrados nos 3 pilares avaliados (Backup Architecture, Cyber Resilient Architecture e Planning and Process). |
| 8 | Construção de Apresentação | Preparação de material de apresentação e realização de apresentação executiva dos resultados. |

3.4.10.14. **RELATÓRIOS E ROADMAP**

3.4.10.15. A CONTRATADA deve disponibilizar a PREFEITURA:

3.4.10.15.1. Relatório Executivo, com uma Visão Comparativa a de Mercado, além dos Impactos no Negócio;

3.4.10.15.2. Relatório Técnico (com o Detalhamento, além das Recomendações, Processos e Tecnologias);

3.4.10.15.3. O estado atual e vantagens da adoção de um modelo resiliente;

3.4.10.15.4. Relatório com o Roadmap de evolução de processos e tecnologia;

3.4.10.15.5. Os planos de curto, médio e longo prazos (conforme viabilidade de execução).

3.4.10.16. **DOCUMENTAÇÃO E APRESENTAÇÃO**

3.4.10.17. A CONTRATADA deverá entregar à PREFEITURA:

3.4.10.17.1. Apresentação dos Resultados, com foco no negócio, processos, tecnologias e serviços. A abordagem deverá garantir a repetibilidade e a consistência usando uma metodologia que torna a segurança dinâmica e adaptável que suporta e permite todas as iniciativas de negócios;

3.4.10.17.2. O Relatório detalhado contendo os principais pontos e o roadmap em PDF;

3.4.10.17.3. O Resumo dos principais pontos encontrados em formato de apresentação em PDF.

3.4.10.18. **OBSERVAÇÕES**:

3.4.10.19. Os relatórios deverão ser entregues em formato de esboço, os documentos serão atualizados e concluídos com base em uma solicitação única de comentários. Será realizada ainda a apresentação dos principais pontos na PREFEITURA ou via conferência virtual, em dia e horário acordados entre a equipe da CONTRATADA e as equipes e partes interessadas (Stakeholders) da PREFEITURA.

3.4.10.20. A PREFEITURA espera da CONTRATADA o fornecimento de no mínimo 550 (quinhentas e cinquenta) horas por Consultor Sênior de Framework de Cibersegurança, além Profissional de Redes Cisco Expert em Cibersegurança (CCIE Security) para o trabalho consultivo previsto no itens 1.3.4.10 durante o período deste Termo.

3.4.10.21. Os serviços deverão ser executados em regime de horário 8x5, ou seja, 8 (oito) horas por 5 (cinco) dias úteis durante a semana.

3.4.11. **GESTÃO DE PROJETOS**

3.4.12. A CONTRATADA deverá prover um responsável pela gestão do serviço, capaz de escalar prioridades e apoiar no agendamento das atividades de consultoria.

## 4. SERVIÇOS TÉCNICOS DE WIFI

### 4.1. PÓS SITE SURVEY

4.1.1. Levantamento de campo, utilizando ferramenta de software especializado, com o objetivo de analisar o ambiente com relação a cobertura de rede sem fio. Poderá ser utilizado para balizar a elaboração de novo projeto de cobertura, projeto de ampliação de cobertura já existente ou avaliar/validar a real condição de cobertura da rede implantada em um determinado local.

4.1.2. Para a realização do Site Survey em ambiente Real, valem todos os requisitos técnicos, normativos e condições estabelecidas, incluindo o uso do software especializado.

4.1.3. Deverá ser elaborado um Relatório de Site Survey, do qual deverão constar:

4.1.3.1. Plano de cobertura e potência dos Pontos de Acesso existentes, utilizando equipamentos instalados no ambiente da PREFEITURA ;

4.1.3.2. Análise da infraestrutura necessária/existente;

4.1.3.3. Validação de cobertura de sinal WIFI e Throughput no ambiente construído, conforme os padrões exigidos pela PREFEITURA , que inclui:

4.1.3.3.1. Relação sinal-ruído (SNR) da cobertura de RF;

4.1.3.3.2. Total de Interferência encontrado;

4.1.3.3.3. Total de Overlap entre os Pontos de Acesso (se disponível);

4.1.3.3.4. Garantia do Throughput no ambiente de Wireless conforme os padrões exigidos pela PREFEITURA;

4.1.3.4. Detecção de Rogues APs;

4.1.3.5. Emissão de Relatório de recomendações de possíveis ajustes (exemplos: possível reposicionamento de Pontos de Acessos ou mesmo aquisição de novos Pontos de Acesso pela PREFEITURA), contendo as seguintes características:

4.1.3.5.1. Fotos;

4.1.3.5.2. Detalhamento;

4.1.3.5.3. Requisitos da Cobertura;

4.1.3.5.4. Conclusão.

4.1.3.6. A CONTRATADA é responsável pelo conhecimento prévio e de todos os requisitos e condições necessárias para realização do Site Survey do tipo Pós, incluindo requisitos específicos de dados e voz sobre WLAN.

4.1.3.7. A CONTRATADA deverá dispor de todos os equipamentos (incluindo Pontos de Acesso), ferramentas e meios de transporte necessários para a realização da atividade.

## 4.2. QUANTIDADE DOS SERVIÇOS

4.2.1. A PREFEITURA estimou os seguintes quantitativos de Site Survey pela CONTRATADA para atender à sua rede Wireless. No entanto, caso entenda ser necessário a adição de novos serviços de Site Survey, serão contratados mais serviços mediante um aditivo comercial com a CONTRATADA.

4.2.2. A tabela a seguir informa a quantidade de serviços previstos durante o período de contrato pela CONTRATADA:

| ITEM | DESCRIÇÃO | ÁREA | QUANTIDADE |
|---|---|---|---|
| 1 | Pós Site Survey | Mínimo 5.000 m2 | 11 |
| 2 | Pós Site Survey | Mínimo 10.000 m2 | 04 |

4.2.3. O prazo do serviço do Pós Site Survey ocorrerá 20 (vinte) corridos após a solicitação da PREFEITURA DE SANTANA DE PARNAÍBA ou conforme cronograma previamente definido em comum acordo com a CONTRATADA.

4.2.4. A PREFEITURA espera que sejam entregues pela CONTRATADA no mínimo 20 (vinte) horas por Site Survey realizado, para atendimento as áreas com no mínimo 5.000 m2.

4.2.5. A PREFEITURA espera que sejam entregues pela CONTRATADA no mínimo 40 (quarenta) horas por Site Survey realizado, para atendimento as áreas com no mínimo 10.000 m2.

4.2.6. A PREFEITURA irá disponibilizar para a CONTRATADA:

4.2.6.1. Envio de planta em formato DWG ou PDF;

4.2.6.2. Definição de área de cobertura/restrição;

4.2.6.3. Finalidade de uso;

4.2.6.4. Informações sobre dispositivos que irão conectar à rede;

4.2.6.5. Permissão para ingresso do notebook de teste à rede do cliente.

4.2.7. Os prazos dos serviços de implantação de infraestrutura deverão estar alinhados com os prazos dos serviços de montagem e configuração correspondentes.

4.3. **OBSERVAÇÕES:**

4.3.1. A CONTRATADA deve considerar o Software Site Survey tais como AirMagnet Survey Pro ou Ekahau, não sendo aceitas soluções OpenSource;

4.3.2. Dispor 2 adaptadores - 2,4/5GHz (Passivo), além de Adaptador mínimo Interno/Suportado com 802.11ac ou 802.11ax (Ativo + Testes de Throughput);

4.3.3. Deverão ser endereçados os Pontos de Acesso em operação nos ambientes indicados pela PREFEITURA;

4.3.4. Deve considerar a controladora Wireless Cisco C9800 em operação na PREFEITURA;

4.3.5. A CONTRATADA deverá utilizar máquina conectada para LAN e Servidor Iperf configurado para receber Tráfego de Upstream e Downstream;

4.3.6. Os serviços de Pós Site Surveys deverão ser realizados presencialmente nas localidades indicadas pela PREFEITURA a CONTRATADA.

4.3.7. Os serviços deverão ser executados em regime de horário 8x5, ou seja, 8 (oito) horas por 5 (cinco) dias úteis.

4.4. **GESTÃO DE PROJETOS**

4.4.1. A CONTRATADA deverá prover um responsável pela gestão do serviço, capaz de escalar prioridades e apoiar no agendamento das atividades de consultoria.

**5. SOLUÇÃO NGFW COM IPS, CONTROLE DE APLICAÇÕES, VPN E AUTENTICAÇÃO MULTIFATOR**

5.1. A solução deverá ser composta de pelo menos 2 (dois) equipamentos do tipo appliance, ou seja, equipamentos produzidos para as funções específicas de Next-Generation Firewall (NGFW) para proteção de perímetro, que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, além de prevenção contra ameaças de vírus, contra malware avançado, e realizar Filtro de URL.

5.2. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.

5.3. Os equipamentos deverão ser idênticos, novos, estarem em produção pelo fabricante, não existindo previsão oficial do modelo ser descontinuado;

5.4. Os equipamentos deverão poder operar em mecanismo de Alta Disponibilidade suportando os modos Ativo-Ativo e Ativo-Passivo;

5.5. Para o funcionamento da solução em Alta Disponibilidade não poderão ser utilizados produtos externos como balanceadores de carga ou similares.

5.6. **CARACTERÍSTICAS DE HARDWARE E DESEMPENHO DE CADA APPLIANCE**

5.6.1. Deve possuir capacidade de processamento de, no mínimo, 10 Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de Firewall, Controle de aplicações, NGIPS e log ativados simultaneamente, considerando-se para fins de métrica, ambientes de produção (1024 Bytes). Este desempenho poderá ser comprovado por meio de documento emitido pelo Fabricante, caso não esteja disponível no Datasheet do produto;

5.6.2. Performance mínima de 05 (cinco) Gbps de Throughput de IPsec VPN;

5.6.3. Deve possuir capacidade de no mínimo 03 (três) Gbps de decriptografia (via Hardware) de TLS v1.2, para inspeção;

5.6.4. Suporte a, no mínimo, 1.500.000 de conexões simultâneas.

5.6.5. Suporte a, no mínimo, 90.000 novas conexões por segundo;

5.6.6. A CONTRATADA poderá comprovar o desempenho dos Firewalls por meio de documentação pública (datasheet) ou apresentar relatório técnico de performance extraído de Ferramenta própria do Fabricante da solução.

5.6.7. Possuir armazenamento interno de, no mínimo, 02 (dois) SSD com capacidade de, no mínimo, 480GB, configurados em RAID 1;

5.6.8. Ter no mínimo 08 (oito) interfaces de rede 10 Gigabit Ethernet (SFP+) ativas e prontas para uso, sem a necessidade de licenciamento adicional;

5.6.9. A CONTRATADA deverá fornecer ao menos 04 (quatro) transceivers modelo 10GBASE-SR ou 10GBASE-SR-S, a serem conectados nas interfaces de cada um dos Firewalls, do mesmo fabricante da solução de Firewall;

5.6.10. A CONTRATADA deverá fornecer cabos do tipo LC-LC, multimodo, com distância de 05 (cinco)

metros, em quantidade suficiente aos transceivers informados;

5.6.11. A Solução deve permitir expansão de interfaces, através de módulos adicionais do mesmo fabricante, permitindo a utilização de no mínimo 08 (oito) interfaces de rede 10 Gigabit Ethernet SFP+ adicionais, além das 8 interfaces 10 Gigabit SFP+ já solicitadas no item 5.6.8;

5.6.12. Deve possuir 02 (duas) fontes de energia AC, redundante e hot-swappable com ajuste automático de tensão para operação nas tensões de 100 a 240-VAC/60 Hz;

5.6.13. Possuir o tamanho máximo de 2U (2 Rack Unit).

5.7. **CARACTERÍSTICAS GERAIS**

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

5.7.2. As funcionalidades de proteção de rede que compõem a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação;

5.7.3. Deverá ser possível acessar o equipamento para aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiverem com alto nível de utilização, através de isolamento entre o processamento de gerenciamento e o processamento do tráfego inspecionado;

5.7.4. 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;

5.7.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

5.7.6. O software deverá ser fornecido em sua versão mais recente (versão recomendada pelo Fabricante) e atualizada;

5.7.7. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS);

5.7.8. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

5.7.8.1. Suporte a 1024 VLAN Tags 802.1q;

5.7.8.2. Agregação de links 802.3ad e LACP;

5.7.8.3. Roteamento multicast (IGMPv1/v2, PIM-SM, Bidir-PIM);

5.7.8.4. DHCP Relay;

5.7.8.5. DHCP Server;

5.7.8.6. Jumbo Frames;

5.7.8.7. Suportar sub-interfaces ethernet lógicas;

5.7.9. Deve suportar os seguintes tipos de NAT:

5.7.9.1. NAT dinâmico (Many-to-1);

5.7.9.2. NAT dinâmico (Many-to-Many);

5.7.9.3. NAT estático (1-to-1);

5.7.9.4. NAT estático (Many-to-Many);

5.7.9.5. NAT estático bidirecional 1-to-1;

5.7.9.6. Tradução de porta (PAT);

5.7.9.7. NAT de Origem;

5.7.9.8. NAT de Destino;

5.7.9.9. Suportar NAT de Origem e NAT de Destino simultaneamente;

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

5.7.9.11. NAT64 e NAT46.

5.7.10. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos e estatísticas de uso das interfaces de rede;

5.7.11. Enviar log para sistemas de monitoração externos, simultaneamente;

5.7.12. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

5.7.13. Proteção anti-spoofing;

5.7.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

5.7.15. Para IPv6, deve suportar roteamento estático e dinâmico;

5.7.16. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

5.7.17. Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

5.7.18. Modo camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

5.7.19. Modo camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

5.7.20. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo:

5.7.20.1. Em modo transparente;

5.7.20.2. Em layer 3;

5.7.21. A configuração em alta disponibilidade deve sincronizar:

5.7.21.1. Sessões;

5.7.21.2. Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;

5.7.22. O HA (modo de alta disponibilidade) deve possibilitar monitoração de falha de link;

5.7.23. A configuração em alta disponibilidade deve possibilitar a instalação de cada membro do cluster, de forma que o sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP);

5.7.24. As características descritas deverão ser passíveis de comprovação por meio de documentação acessível no site do fabricante na Internet;

5.8. **CONTROLE POR POLÍTICA DE FIREWALL**

5.8.1. Deve suportar controles por zona de segurança;

5.8.2. Deve suportar controles de políticas por porta e protocolo;

5.8.3. Deve suportar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

5.8.4. Deve ter suporte a controle de políticas por usuários, grupos de usuários (Microsoft AD), IPs, redes e zonas de segurança;

5.8.5. Deve suportar controle de políticas por país (geolocation);

5.8.6. Deve suportar controle, inspeção e decriptografia de SSL por política para tráfego de entrada

(inbound) e Saída (outbound);

5.8.7. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (inbound);

5.8.8. Deve realizar decriptografia tráfego inbound e outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

5.8.9. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, zip, tar, mp3, scr, cpl, ocx, pif, class, jar, chm, hlp, vbe, hta, wsf, torrent, 7z, rar, flash, tar, msi, rar;

5.8.10. Suporte a objetos e regras IPV6;

5.8.11. Suporte a objetos e regras multicast;

5.8.12. Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: drop sem notificação do bloqueio ao usuário, drop com notificação do bloqueio ao usuário, TCP-Reset para o client, TCP-Reset para o server ou para ambos os lados da conexão;

5.8.13. Deve suportar filtragem de URL:

5.8.14. A plataforma de segurança deve suportar as seguintes funcionalidades de filtro de URL:

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

5.8.14.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

5.8.15. Deve ter suporte as seguintes funcionalidades de filtro de URL:

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

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

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

5.8.15.4. Deve suportar ter uma base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

5.8.15.5. Possuir suporte a ao menos 80 categorias de URLs;

5.8.15.6. Permitir a criação de categorias de URLs customizadas;

5.8.15.7. Suportar a função de exclusão de URLs do bloqueio, por categoria;

5.8.15.8. Ter suporte a customização de página de bloqueio;

5.8.15.9. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

5.8.15.10. Suportar popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

5.8.15.11. Ter suporte a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

5.8.15.12. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

5.8.15.13. Suporte a criação categorias de URLs customizadas;

5.8.15.14. Suporta a exclusão de URLs do bloqueio, por categoria;

5.8.15.15. Deve permitir a customização de página de bloqueio.

5.9. **CONTROLE DE APLICAÇÕES**

5.9.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independentemente de porta e protocolo, com as seguintes funcionalidades:

5.9.1.1. Deve ser possível a liberação e bloqueio exclusivo de aplicações sem a necessidade de liberação de portas e protocolos;

5.9.1.2. Deve ter capacidade de reconhecer pelo menos 3.000 (três 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;

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

5.9.2. Deve inspecionar o payload de pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo;

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

5.9.4. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde à especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;

5.9.5. Deve identificar o uso de táticas evasivas via comunicações criptografadas;

5.9.6. Deve atualizar a base de assinaturas de aplicações automaticamente;

5.9.7. Deve limitar a banda (download/upload) usada por aplicações (rate limiting) baseado no IP de origem, usuários e grupos do LDAP/AD;

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

5.9.9. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente à possibilidade de habilitar controle de aplicações em algumas regras;

5.9.10. Deve suportar, no mínimo, os seguintes métodos de identificação e classificação das aplicações:

5.9.10.1. Checagem de assinaturas e decodificação de protocolos;

5.9.10.2. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

5.9.10.3. Deve 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, mantendo a confidencialidade das aplicações do ambiente do PREFEITURA ;

5.9.11. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares e contexto

(sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de, pelo menos, os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

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

5.9.13. Deve alertar o usuário quando uma aplicação for bloqueada;

5.9.14. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

5.9.15. Deve possibilitar a diferenciação de tráfegos Peer2Peer (ex.: Bittorrent, emule, neonet), possuindo granularidade de controle/políticas para os mesmos;

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

5.9.17. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o uso do chat e bloquear a chamada de vídeo.

5.10. **PREVENÇÃO DE AMEAÇAS (NGIPS)**

5.10.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrado ao appliance de Firewall;

5.10.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos;

5.10.3. Deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo;

5.10.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

5.10.5. Deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão;

5.10.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura;

5.10.7. Deve suportar elephant flows (conexões de fluxo TCP (ou outro protocolo) com fluxo contínuo grande em bytes totais de longa duração);

5.10.8. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens:

5.10.8.1. Deve permitir o bloqueio de vulnerabilidades;

5.10.8.2. Deve permitir o bloqueio de exploits conhecidos;

5.10.8.3. Deve incluir proteção contra-ataques de negação de serviços;

5.10.8.4. Deve possuir os seguintes mecanismos de inspeção de IPS:

5.10.8.4.1. Análise de padrões de estado de conexões;

5.10.8.4.2. Análise de decodificação de protocolo;

5.10.8.4.3. Análise para detecção de anomalias de protocolo;

5.10.8.4.4. IP Defragmentation;

5.10.8.4.5. Remontagem de pacotes de TCP;

5.10.8.4.6. Bloqueio de pacotes malformados;

5.10.8.4.7. Deve ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

5.10.9. Deve detectar e bloquear a origem de portscans;

5.10.10. Suportar Eventos de Indicadores de Comprometimento (IoCs), tais como Malware backdoors, IP´s de C2 (Command and Control) em DNS Servers, URLs supeitas, além de “samples” de Malware conhecidos (malwares já executados, arquivos de Office, PDF, Java comprometidos, etc.)

5.10.11. Deve bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

5.10.12. Deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

5.10.13. Deve possuir assinaturas para bloqueio de ataques de buffer overflow;

5.10.14. Deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

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

5.10.16. Deve permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

5.10.17. Deve suportar bloqueio de arquivos por tipo;

5.10.18. Deve identificar e bloquear comunicação com botnets;

5.10.19. Deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

5.10.19.1. Nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

5.10.20. Deve suportar a captura de pacotes (PCAP) por assinatura de IPS e controle de aplicação;

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

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

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

5.10.24. Deve oferecer proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos;

5.10.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseada 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 e zonas de segurança;

5.10.26. Deve permitir, criar ou importar regras no padrão OpenSource (SNORT), sendo que essas regras devem poder ser habilitadas para simples monitoramento ou para bloqueio de tráfego, não havendo limite na quantidade de regras a serem criadas ou importadas e não deve haver limite de funcionalidade nas regras criadas ou a serem importadas;

5.10.27. Deve permitir a análise do comportamento da rede fornecendo visibilidade do uso do segmento monitorado para auxiliar na solução de falhas de rede ou degradação de desempenho, no mínimo as seguintes informações devem ser disponibilizadas:

5.10.27.1. Fluxos de sessão dos hosts;

5.10.27.2. Hora de início/fim;

5.10.27.3. Quantidade de dados trafegados;

5.10.27.4. Deve permitir coletar, armazenar e correlacionar as informações adquiridas passivamente, sobre hosts que trafegam pelos segmentos monitorados pelo(s) IPS. No mínimo as seguintes informações devem ser correlacionadas e armazenadas:

5.10.27.5. Sistema operacional ou IP do Host;

5.10.27.6. Serviços existentes ou ID da sessão no Host;

5.10.27.7. Portas em uso no Host;

5.10.27.8. Aplicações em uso no Host;

5.10.27.9. Vulnerabilidades existentes no Host;

5.10.27.10. Identidades de usuários;

5.10.27.11. Tipo de arquivo e protocolo;

5.10.27.12. Conexões maliciosas

5.10.28. Deve implementar funcionalidade de Análise de Tráfego de Redes (Network Detection and Response - NDR), que através de Machine Learning detecta anomalias de rede e ameaças de malware, sem realizar a decriptação do pacote de dados. A solução deve ser capaz de:

5.10.28.1. Trazer visibilidade em arquivos/pacotes com criptografia TLS ou QUIC sem decriptá-los;

5.10.28.2. Detectar Ataques encriptados, procurando pela presença de campanhas web maliciosas visitadas, cifras mais fracas, protocolos vulneráveis, invasões de rede e ataques baseados em botnet;

5.10.28.3. Suportar string de impressão digital calculada a partir de campos dos pacotes;

5.10.28.4. Utilizar aprendizado de máquina (ML) para determinar a aplicação (processo cliente);

5.10.28.5. Identificar processos conhecidos e aplicações clientes;

5.10.28.6. Executar ações com base em Políticas implementadas (permitir, bloquear, inspecionar, etc.) disponíveis com base na aplicação;

5.10.28.7. Identificar malwares com base em impressões digitais seguras via Analíticos.

5.10.29. Caso a funcionalidade descrita no item 7.3.10.27 não esteja disponível diretamente no Firewall, a CONTRATADA poderá compor com solução adicional de NDR (Network Detection and Response), sendo que deverá fornecer o devido hardware e software necessários em Alta disponibilidade, bem como garantir a devida integração (via chamadas de API) aos NGFWs ofertados, além de todo o suporte devido durante o contrato vigente, sem qualquer ônus à PREFEITURA.

5.11. **ANÁLISE DE MALWARE**

5.11.1. Devido ao malware, hoje em dia, ser muito dinâmico e um antivírus comum reativo não ser capaz de detectá-los com a mesma velocidade que suas variações são criadas, a solução ofertada deverá possuir funcionalidades para análise de malware não conhecido, incluídas na própria ferramenta ou entregues mediante composição com outro fabricante;

5.11.2. Deve suportar operação em ambientes configurados para alta disponibilidade;

5.11.3. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados para análise "in Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

5.11.4. Deve permitir de forma automática a criação e manutenção de um histórico ou fluxo de trabalho forense no qual seja possível identificar:

5.11.4.1. Capacidade de inspeção de malware no ambiente de rede, mesmo quando não seja detectado

inicialmente como malware, e movimento lateral;

5.11.4.2. Deve permitir selecionar, através de políticas granulares, quais tipos de arquivos sofrerão esta análise, incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente.

5.11.5. Deve suportar a monitoração, detecção e prevenção, em tempo real, de arquivos trafegados nos seguintes protocolos: FTP, HTTP, SMTP, IMAP, POP3, como também arquivos trafegados internamente entre servidores de arquivos usando SMB, em todos os modos de implementação: transparente e L3;

5.11.6. Deve permitir especificar o tipo de arquivo, inclusive os comprimidos, que serão analisados em cada política de controle de malware, permitindo especificar um contexto de análise para redes, VLANs e outros objetos associados ao controle de acesso do ambiente protegido;

5.11.7. Deve permitir que seja definido o tamanho máximo dos arquivos a serem inspecionados;

5.11.8. Deve utilizar mecanismo de proteção baseado em reputação global em tempo real, permitindo que sejam adotadas ações automáticas de alerta e bloqueio de arquivos suspeitos ou malware já encontrado anteriormente;

5.11.9. O dispositivo não deve depender ou utilizar de forma exclusiva mecanismos de análise em ambiente virtualizado para que seja feita a detecção e o bloqueio de malware em tempo real;

5.11.10. A utilização de recursos de execução virtualizada não deve depender da configuração manual de imagens ou escolha de versões específicas de sistemas operacionais;

5.11.11. Deve possui mecanismo blacklist para implementar controles customizados de forma automatizada;

5.11.12. Deve possui mecanismo whitelist para implementar controles customizados de forma automatizada;

5.11.13. Deve possui capacidade para detecção de malware em comunicações de entrada e saída, incluindo a detecção de mecanismos de Comando e Controle;

5.11.14. Deve identificar ataques como: ataques direcionados, zero day, exploração de vulnerabilidades, indicadores de obfuscação e indicadores de comprometimento automático;

5.11.15. Deve possuir tecnologia proprietária de execução para verificação de malware avançado, inclusive mecanismos tipo sandbox;

5.11.16. Deve implementar a identificação e capacidade de controle de acesso em tempo real por tipo de arquivo. Adicionalmente, deve implementar em tempo real a inspeção, detecção e bloqueio autônomo (prevenção sem a necessidade de integrar com sistemas de terceiros para que seja feito o bloqueio da ameaça) na rede por tipo de arquivo.

5.11.17. Deve implementar atualização a base de dados da rede de inteligência de forma automática;

5.11.18. Para recurso de análise virtualizada existente, deve ser mantido um histórico dos resultados de avaliações prévias de um arquivo e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite;

5.11.19. Deve dispor de múltiplos motores e mecanismos de detecção e prevenção para verificação de malware e códigos maliciosos devendo possuir no mínimo 3(três) dos listados abaixo:

5.11.19.1. Machine learning;

5.11.19.2. Reputação global;

5.11.19.3. Detecção customizada local por blacklist e regras customizadas de detecção de tráfego de rede;

5.11.19.4. Análise estática;

5.11.19.5. Análise dinâmica (sandbox).

5.11.20. O processo de análise de comunicações, malware e sua prevenção deve ocorrer em tempo real, não sendo aceitas tecnologias que dependam de verificações que induzam latência suficiente para postergar a entrega de arquivos ao seu destino original;

5.11.21. Deve permitir o download de malware identificado a partir da própria interface de gerência;

5.11.22. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 10 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

5.11.23. Caso sejam necessárias licenças de sistema operacional e software para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para o PREFEITURA;

5.11.24. Deve suportar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado;

5.11.25. Deve suportar a análise de arquivos do pacote Microsoft Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e arquivos java (.jar e .class);

5.11.26. Deve permitir o envio de arquivos para análise no ambiente controlado de forma automática.

5.12. **IDENTIFICAÇÃO DE USUÁRIOS**

5.12.1. 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, Microsoft Active Directory e base de dados local;

5.12.2. Deve permitir integração (nativa ou através de software complementar do mesmo Fabricante) com o Microsoft Active Directory, para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.12.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Microsoft Windows Server 2012 R2 e versões superiores;

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

5.12.5. Deve permitir o controle, sem instalação de software cliente, em equipamentos que solicitem saída para Internet, para que antes de iniciar a navegação, seja exibido um portal de autenticação hospedado no firewall (Captive Portal);

5.13. **FILTRO DE DADOS**

5.13.1. Deve permitir a criação de filtros para arquivos e dados pré-definidos;

5.13.2. Os arquivos devem ser identificados por extensão e assinaturas;

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

5.13.4. Deve suportar a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

5.13.5. Deve suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

5.13.6. Deve 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;

5.14. **GEO-LOCALIZAÇÃO**

5.14.1. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado país/países seja bloqueado;

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

5.14.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

5.15. **PLATAFORMA DE CONSOLE DE GERÊNCIA**

5.15.1. Características técnicas mínimas:

5.15.1.1. Deve ser do mesmo fabricante que dos Firewalls

5.15.1.2. A solução ofertada deverá ser entregue com virtual appliance compatível com Nutanix AHV e VMware para gerenciamento centralizado do cluster NGFW ofertado.

5.15.2. As funcionalidades de gerência e retenção de logs que compõem a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação;

5.15.3. A console de Gerência deve ser capaz de armazenar um mínimo de 250 (duzentos e cinquenta) GB de armazenamento de logs.

5.15.4. A solução deve ser capaz de armazenar o equivalente a 2TB de logs por meio de Upgrade.

5.15.5. A solução deve ser capaz de exportar os logs em um servidor syslog dedicado ou SIEM.

5.15.6. A console de Gerência deverá ter capacidade para gerenciar e monitorar um mínimo 2000 (dois mil) acessos remotos VPN ou Endpoints.

5.15.7. Deve centralizar logs e relatórios usando uma única interface de gerenciamento;

5.15.8. Não será permitida a instalação de cliente para administração do appliance de firewall;

5.15.9. O gerenciamento deve permitir/possuir:

5.15.9.1. Visualização de logs e relatórios relacionados às políticas de firewall e controle de aplicação;

5.15.9.2. Visualização de logs e relatórios relacionados ao IPS, Controle de Aplicação e Anti-Malware;

5.15.9.3. Visualização de logs e relatórios relacionados às políticas de Filtro de URL;

5.15.9.4. Monitoração de logs;

5.15.9.5. Ferramentas de investigação de logs;

5.15.9.6. Visualização das capturas de pacotes realizadas nos ataques detectados.

5.15.10. Acesso concorrente de administradores;

5.15.11. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

5.15.12. Deve suportar a definição de perfis de acesso à console, com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

5.15.13. Deve suportar autenticação integrada ao Microsoft Active Directory (AD) e servidor RADIUS;

5.15.14. Deve possibilitar a geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

5.15.15. Deve possuir integração nativa com plataforma de proteção de cargas de trabalho (cwpp) para enviar contexto para detectar e realizar a quarentena de hosts infectados na rede;

5.15.16. Deve ter capacidade de gerar relatórios gráficos que permitam visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, permitindo comparar os diferentes consumos realizados pelas aplicações no decorrer do tempo;

5.15.17. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spyware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

5.15.18. Deve permitir a criação de painéis (dashboards) ou relatórios customizados com, no mínimo, as seguintes informações: visibilidade do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, malware detectado, aplicações mais utilizadas, protocolos mais utilizados, principais atacantes (com informação de geolocalização);

5.15.19. Deve possibilitar a coleta de estatísticas de todo o tráfego associado aos dispositivos de segurança;

5.15.20. Deve prover uma visualização sumarizada das aplicações e URLs que geraram tráfego associado à solução;

5.15.21. Deve possuir mecanismo "drill-down" para navegação nos dashboards em tempo real;

5.15.22. Deve ser possível exportar os logs em CSV;

5.15.23. Deve permitir que os logs e relatórios sejam rotacionados automaticamente em função do tempo em que estão armazenados na solução;

5.15.24. Deve exibir as seguintes informações, de forma histórica ou em tempo real:

5.15.24.1. Situação do dispositivo e do cluster;

5.15.24.2. Principais aplicações;

5.15.24.3. Principais aplicações por risco;

5.15.24.4. Principais ameaças;

5.15.24.5. Uso de CPU e memória;

5.15.24.6. Hosts mais acessados (hit count);

5.15.24.7. Usuários que mais estão utilizando largura de banda de entrada e saída.

5.15.25. No mínimo, os seguintes relatórios devem ser gerados:

5.15.25.1. Resumo gráfico de aplicações utilizadas;

5.15.25.2. Principais aplicações por utilização de largura de banda de entrada e saída;

5.15.25.3. Principais aplicações por taxa de transferência de bytes;

5.15.25.4. Principais hosts por número de ameaças identificadas.

5.15.26. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL e ameaças de rede vinculadas a este tráfego;

5.15.27. Deve permitir a criação de relatórios personalizados;

5.15.28. Deve gerar alertas automáticos via:

5.15.28.1. Email;

5.15.28.2. SNMP;

5.15.28.3. Syslog.

5.15.29. O gerenciamento deve permitir/possuir:

5.15.29.1. Criação e administração de políticas de firewall e controle de aplicação;

5.15.29.2. Criação e administração de políticas de IPS e Anti-Malware;

5.15.29.3. Criação e administração de políticas de Filtro de URL;

5.15.29.4. Uso de palavras chaves para facilitar identificação de regras;

5.15.29.5. Alertas de alterações, no caso acesso simultâneo de dois ou mais administradores.

5.15.30. Definição de perfis de acesso à console com permissões granulares como:

5.15.30.1. Acesso de escrita, acesso de leitura, criação de usuários e alteração de configurações;

5.15.30.2. Autenticação integrada ao Microsoft Active Directory (AD) e servidor Radius;

5.15.30.3. Localização das regras em que um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

5.15.30.4. Backup das configurações e rollback de configuração para a última configuração salva;

5.15.30.5. Mecanismo de validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras.

5.15.31. Visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

5.16. **SOLUÇÃO DE CLIENTES VPN (VIRTUAL PRIVATE NETWORK)**

5.16.1. A plataforma de VPN deve fornecer uma experiência de conectividade segura através de uma vasta gama de PCs, Laptops e Dispositivos móveis. Deve fornecer o Serviço de VPN contínuo e inteligente, que habilita VPN via um cliente instalado para automaticamente selecionar a rede mais adequada e adaptar o seu protocolo de tunelamento com o método mais eficiente de conexão.

5.16.2. CARACTERÍSTICAS DE SOFTWARE

5.16.2.1. A funcionalidade de VPN deve ser entregue via licenças como subscrição.

5.16.2.1.1. Deve implementar SSL VPN Client-to-site e fornecer licenças para um mínimo de 2500 (duas mil e quinhentas) licenças usuários simultâneos/conexões remotas VPN.

5.16.2.1.2. A CONTRATADA deverá fornecer os arquivos de instalação ou de imagem (OVA ou similar), em caso de appliance virtual, de maneira eletrônica, além dos arquivos ou chaves de licenças a serem instalados na solução. Também fornecer procedimento de transferência das licenças para outro equipamento (rehost) em caso de necessidade futura.

5.16.2.2. Deve suportar VPN Site-to-Site;

5.16.2.3. Deve suportar IPSec VPN;

5.16.2.4. A VPN IPSEc deve suportar no mínimo:

5.16.2.4.1. Autenticação MD5 e SHA-1;

5.16.2.4.2. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

5.16.2.4.3. Algoritmo Internet Key Exchange (IKEv1 e v2);

5.16.2.4.4. AES 128, 192 e 256 (Advanced Encryption Standard);

5.16.2.4.5. Autenticação via certificado IKE PKI;

5.16.2.5. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

5.16.2.6. Deve suportar SSL ou IPSec para “remote access VPN”;

5.16.2.7. Permitir opções de autenticação Flexíveis, utilizando chaves automáticas (pre-shared key) e certificados;

5.16.2.8. Suportar monitorar o uso de aplicativos dos Endpoints para descobrir possíveis anomalias de comportamento e tomar decisões de serviço e design de segurança de rede;

5.16.2.9. A autenticação do acesso do cliente poderá ser feita via AD, permitindo o usuário trocar a senha expirada através do próprio cliente de VPN.

5.16.2.10. Se capaz de enviar contextos (telemetria) para a Plataforma de Proteção de Workloads (WPP) para enriquecer o controle de segurança feito por ela. Caso a solução não tenha essa capacidade, a CONTRATADA poderá realizar o desenvolvimento desta integração (via SDK ou APIs) com a Solução de Plataforma de Proteção de Workloads (WPP) oferecida, considerando não só o desenvolvimento, mas também a sustentação do ambiente [suporte] durante o período de contrato.

5.16.2.11. Compatibilidade com sistemas operacionais Clientes:

5.16.2.11.1. Software Remote Access

16.2.11.1.1. Deve suportar Windows 7/8.1/10, macOS 10.13, 10.14.

5.16.2.11.2. Aplicativos Móveis

16.2.11.2.1. Deve suportar Android 4+, iOS 5.0 e posteriores ou ChromeOS

5.16.2.11.3. Navegadores: SSL VPN.

16.2.11.3.1. Deve suportar Windows, macOS, iOS, Android e Linux.

5.16.2.12. Deve ser capaz de verificar a postura dos dispositivos, conforme as políticas de segurança definidas pelo Serviço de Autenticação (NAC). A CONTRATADA poderá realizar o desenvolvimento desta integração (via SDK ou APIs) com a Solução de Autenticação (NAC) ofertada, que inclui o desenvolvimento e a sustentação do ambiente [suporte] durante o período vigente de contrato.

5.16.2.13. Ter a capacidade de também servir como cliente da solução de EDR (Endpoint, Detection and Remediation), sem a necessidade desta solução instalar um novo cliente dedicado. A CONTRATADA poderá realizar o desenvolvimento desta integração (via SDK ou APIs) com a Solução EDR ofertada, que inclui o desenvolvimento e a sustentação do ambiente [suporte] durante o período vigente de contrato.

5.17. **SOLUÇÃO DE MÚLTIPLO FATOR DE AUTENTICAÇÃO**

5.17.1. HARDWARE E SOFTWARE

5.17.1.1. A Solução deve ser entregue no modelo de Software como Serviço (SaaS);

5.17.1.2. Deve ser entregue com capacidade para no mínimo 2500 (duas mil e quinhentas) licenças;

5.17.1.3. Todo o licenciamento com subscrição deve ser ter validade mínima de 48 (quarenta e oito) meses;

5.17.1.4. A CONTRATADA prestará serviço especializado para implantação, integração, configuração e ativação da solução de múltiplo fator de autenticação, no ambiente da PREFEITURA;

5.17.1.5. A CONTRATADA prestará serviço especializado de suporte técnico da solução de múltiplo fator de autenticação, no ambiente da PREFEITURA.

5.17.2. **ESPECIFICAÇÃO TÉCNICA DO OBJETO**

5.17.2.1. Aquisição de solução para múltiplo fator de autenticação, considerando a descrição abaixo:

5.17.2.1.1. A CONTRATADA prestará serviço especializado para implantação, configuração e ativação da solução de múltiplo fator de autenticação, no ambiente da CONTRATANTE.

5.17.2.1.2. A CONTRATADA prestará serviço especializado de suporte técnico da solução de múltiplo fator de

autenticação, no ambiente da CONTRATANTE, sem custos adicionais.

5.17.2.1.3. A CONTRATADA prestará o treinamento especializado da solução de múltiplo fator de autenticação, nas dependências da CONTRATANTE, sem custos adicionais.

5.17.3. **INTEGRAÇÕES**

5.17.3.1. A solução deve permitir a autenticação de usuários com múltiplo fator para os seguintes ambientes e produtos:

5.17.3.1.1. Solução de VPN em estações de trabalho e dispositivos móveis com sistema operacional Android, iOS e Windows, no mínimo. A solução deve permitir que o servidor de VPN obtenha a lista de grupos autorizados para o usuário a partir do diretório de autenticação.

5.17.3.1.2. Microsoft Remote Desktop Protocol – RDP, com o uso do Microsoft Remote Desktop Gateway.

5.17.3.1.3. Microsoft Remote Desktop Protocol – RDP, sem o uso do Microsoft Remote Desktop Gateway.

5.17.3.1.4. Estações de trabalho Microsoft Windows 10 e superiores.

5.17.3.1.5. Servidores Windows 2012 R2 e superiores.

5.17.4. **PREMISSAS E REQUISITOS TÉCNICOS**

5.17.4.1. A solução fornecida deverá possuir funcionalidade que permita compartilhar os logs, em tempo real e/ou por agendamento, com a ferramenta de SIEM – Security Information Event Management.

5.17.4.2. Em caso desta funcionalidade utilizar componentes externos, a CONTRATADA deverá entregar, instalar, configurar e suportar e atualizar os respectivos componentes durante a vigência do contrato. A licença de uso dos componentes deverá ser válida durante a vigência contratual.

5.17.4.3. Caso a solução da CONTRATADA não possua integração nativa, a CONTRATADA deve fornecer os métodos para leitura, interpretação e normalização dos dados, com seus respectivos parsers (expressões regulares), para leitura adequada das variáveis presentes nas logs da solução. A CONTRATADA deve entregar, manter, suportar e atualizar estes métodos, durante a vigência do contrato. A licença de uso dos métodos utilizados deve estar contemplada na assinatura. A PREFEITURA reserva-se, ao seu critério, o direito de utilizar os métodos que considerar mais adequados.

5.17.4.4. A solução deverá possibilitar que as conexões de saída para a internet sejam realizadas através de servidor de proxy.

5.17.4.5. A solução deverá possuir mecanismos de contingência para que, caso ocorra a interrupção da conexão de internet ou indisponibilidade do serviço da CONTRATADA, os usuários possam continuar se autenticando no ambiente da PREFEITURA.

5.17.4.6. A solução deverá ter capacidade de avisar o usuário, quando ocorrer algum erro, através de mensagens que ajudem a identificar a causa sem expor informações críticas.

5.17.4.7. A solução deverá possuir capacidade de integração com o Security Assertion Markup Language - SAML.

5.17.4.8. A solução deverá possuir capacidade de integração com Remote Authentication Dial-In User Service - RADIUS.

5.17.4.9. A solução deverá possuir capacidade de disponibilizar pelo menos os seguintes fatores de autenticação:

5.17.4.9.1. Push Notification (Notificação enviada para app instalado no dispositivo do usuário);

5.17.4.9.2. Software Token – OTP (One Time Password):

5.17.4.9.3. OTP enviado por e-mail;

5.17.4.9.4. OTP enviado por Short Message Service - SMS.

5.17.4.10. A solução deverá possuir capacidade de permitir criação de políticas para definir quais usuários terão obrigatoriedade de utilização de múltiplo fator de autenticação.

5.17.4.11. A solução deverá possuir capacidade de permitir criação de políticas baseadas no comportamento do usuário para permitir o acesso ou não ao ambiente da PREFEITURA, pelo menos para os seguintes itens: localização do usuário, endereço IP de origem, horário de acesso, avaliação de segurança (saúde) do dispositivo utilizado para aprovação.

5.17.4.12. A solução deverá ser compatível, com no mínimo, os navegadores Microsoft Internet Explorer 11, Microsoft Edge e/ou Google Chrome 75 ou superior, esta por sua vez, também deve ser compatível com navegadores de dispositivos móveis com sistema operacional Android e iOS no mínimo.

5.17.4.13. Caso necessário cadastrar e-mail de usuário na solução da CONTRATADA, o endereço deve ser exclusivamente exclusivamente do domínio: @santanadeparnaiba.sp.gov.br ou outro informado pelo PREFEITURA, sem possibilidade de ser alterado pelo usuário.

5.17.4.14. A solução deverá desconectar a interface de administração quando houver período de tempo definido sem atividade;

5.17.4.15. A solução deve permitir que os usuários possam optar, a cada autenticação, por acessar estações de trabalho e servidores Microsoft Windows através de uma das formas abaixo:

5.17.4.16. Utilizando cartão inteligente com certificado x.509 protegido por senha (PIN), solução já utilizada no ambiente da CONTRATANTE, sem a exigência de fator de autenticação adicional da solução;

5.17.4.17. Utilizando conta e senha do Active Directory, com a exigência de fator de autenticação adicional da solução.

5.17.4.18. Para que ocorra a integração da solução ao ambiente da CONTRATANTE é necessário que os requisitos técnicos abaixo sejam atendidos sem comprometer a atual infraestrutura da CONTRATANTE:

5.17.4.19. A solução poderá utilizar recursos em nuvem, assim como componentes instalados no ambiente da CONTRATANTE.

5.17.4.20. Caso seja necessário instalar parte da solução nas dependências da CONTRATANTE a CONTRATADA deverá seguir as seguintes especificações:

5.17.4.21. Servidores Virtuais para aplicações, software básico:

5.17.4.21.1. Servidores Virtuais ou appliance em ambiente VMware 6.5 ou superior.

5.17.4.21.2. Sistema Operacional Windows 2016 e superior preferencialmente Windows Server 2019:

17.4.21.2.1. Microsoft IIS 10 e superior.

17.4.21.2.2. Microsoft .NET Framework 4.7 ou superior.

17.4.21.2.3. Sistema Operacional Oracle Linux versão 7 releases atual e superiores.

5.17.4.22. Para o caso de a solução ser homologada para Oracle Linux 7 release atual ou superior, a CONTRATANTE já possui suporte da Oracle.

5.17.4.23. Para caso a solução tenha que utilizar Red Hat 7 release atual e superior ou JBoss EAP, é necessário ter subscrições e suporte da Red Hat para os servidores, fornecidos pela CONTRATADA, durante a vigência

do contrato.

5.17.4.24. Serão aceitos os pré-requisitos de software como Apache, OpenJDK ou TomCat apenas para versões nativas do release da distribuição. Caso faça uso de alguma versão diferente, a mesma deve ser empacotada junto à solução e suportada pelo fabricante, como parte integrante do produto, sob total responsabilidade da CONTRATADA.

5.17.4.25. As bibliotecas e aplicações de sistema operacional devem ser padrão da versão e release, com pacotes oriundos dos repositórios oficiais.

5.17.4.26. Caso a solução seja conteinerizada em arquitetura de microsserviços, deve utilizar a arquitetura Red Hat OpenShift. Se a aplicação utilizar contêineres em arquitetura monolítica deve ser compatível com o Docker da Oracle.

5.17.4.27. A solução deve executar em servidores virtuais preferencialmente distribuídos e balanceados entre dois data centers, na modalidade ativo/ativo.

5.17.4.28. A solução que não suportar a modalidade ativo/ativo deverá executar em um servidor virtual e ter a sua contingência implementada entre sites pela facilidade HA (High Availability) da VMware. A solução deve oferecer suporte a vMotion.

5.17.4.29. O número de servidores que compõe a solução não pode ser superior a 5. Este número pode, no entanto, chegar a 10 (dez) servidores, caso todos os componentes utilizem a modalidade ativo/ativo distribuídos entre dois data centers.

5.17.4.30. Caso a solução utilize algum servidor físico, o mesmo deverá ser fornecido junto com a solução assim como o suporte ao hardware e as licenças de softwares necessárias.

5.17.4.31. Caso a solução faça uso de Java, deve estar incluso o licenciamento de Java para todos os servidores da solução.

5.17.4.32. A instalação de componentes ou agentes da solução em servidores da CONTRATANTE não pode acarretar na perda do suporte da plataforma a qual foi integrada.

5.17.4.33. A CONTRATADA deverá possuir licença válida da solução durante a vigência do contrato.

5.17.4.34. A solução deverá ser mantida atualizada, priorizando as atualizações de segurança.

5.17.4.35. Caso necessária atualização ou manutenção, esta deve ser acordada previamente com a CONTRATANTE a fim de evitar indisponibilidades e comprometimento da solução.

5.17.4.36. As atualizações e manutenções realizadas no ambiente não devem impactar em configurações e adequações já realizadas.

5.17.4.37. A CONTRATADA deverá fornecer canais de atendimento e suporte à solução através de abertura de chamados em seu website, por e-mail ou telefone sem gerar ônus a CONTRATANTE.

5.17.4.38. A solução deverá permitir portabilidade de informações, dados, base de conhecimento e configurações, nos formatos: CSV, XML, PDF ou outro formato de arquivo estruturado.

5.17.4.39. A solução deverá armazenar de forma segura as senhas de contas de administradores não sincronizadas com diretório (AD/LDAP) definido pela CONTRATANTE.

5.17.4.40. A solução deverá ser acessível para os administradores da solução, via interface web e não necessitar de complementos, plug-ins ou extensões para seu pleno funcionamento.

5.17.5. **CARACTERÍSTICAS GERAIS DA SOLUÇÃO**

5.17.5.1. A CONTRATADA deverá realizar a transferência de conhecimento da solução para a

CONTRATANTE, conforme o Plano de Treinamento, no máximo até o ultimo dia antes de finalizar a implantação da solução, no ambiente da CONTRATANTE.

5.17.5.2. A solução deverá possuir documentação de suporte com informações da solução.

5.17.5.3. A solução deverá possuir manual, acessível para consulta, durante vigência do contrato.

5.17.5.4. Os dados inseridos na solução para atendimento deste contrato são de propriedade da CONTRATANTE.

5.17.5.5. Quando do encerramento ou rescisão do contrato, os dados inseridos na solução deverão passar por processo de descarte seguro.

5.17.6. **CONTROLE DE ACESSOS**

5.17.6.1. A solução deverá permitir a criação de diferentes perfis de usuários, com diferentes níveis de autorização, permissões e visões, garantindo que as permissões de acesso sejam gerenciadas a partir da interface da solução da CONTRATADA.

5.17.6.2. A solução deverá possuir suporte à integração Single Sign On - SSO, permitindo a autenticação na interface de administração utilizando recursos de federação, através do uso de Security Assertion Markup Language – SAML. Neste cenário deve ser possível exigir fator adicional de autenticação da solução.

5.17.6.3. A solução deverá possuir recurso para o provisionamento e desprovisionamento dos usuários, devendo ser utilizada a integração e sincronização com o serviço de diretório AD e/ou LDAP da CONTRATANTE ou através de chamadas de API pela CONTRATANTE.

5.17.6.4. A solução deverá permitir que somente usuários administradores devam ser capazes de criar, alterar ou remover usuários e suas permissões associadas conforme perfis.

5.17.6.5. Para o provisionamento das autorizações de acesso dos usuários na interface de administração da solução da CONTRATADA, deverá ser utilizada uma das seguintes alternativas:

5.17.6.5.1. Integração com o serviço de diretório AD ou LDAP da CONTRATANTE: a associação de usuários aos grupos de usuários (perfis) deve ser obtida do serviço de diretório AD ou LDAP da CONTRATANTE.

5.17.6.5.2. A solução deverá suportar múltiplos domínios de Microsoft Active Directory.

5.17.6.5.3. A solução deverá suportar a utilização pelo usuário para autenticação em múltiplos dispositivos, com no mínimo os sistemas operacionais Windows, Android e iOS.

5.17.6.6. A solução deverá implementar capacidade de permitir criação de políticas baseadas no comportamento do usuário e na avaliação do dispositivo para permitir o acesso ou não ao ambiente da PREFEITURA, pelo menos para os seguintes itens e verificações:

5.17.6.6.1. Localização do usuário;

5.17.6.6.2. Endereço IP de origem;

5.17.6.6.3. Horário de acesso.

5.17.6.6.4. Histórico do dispositivo (se é o dispositivo comumente utilizado para a autenticação);

5.17.6.6.5. Versão do sistema operacional do dispositivo (se está atualizado);

5.17.6.6.6. Bloqueio de tela (verificar se o dispositivo possui bloqueio de tela protegido por senha) ou o aplicativo da solução possuir a possibilidade de solicitação de uma senha (pin) para acessá-lo.

5.17.6.6.7. Dispositivo com jailbroken ou rooted.

5.17.6.7. A solução não deve permitir que o usuário remova a exigência do uso do fator adicional da solução.

5.17.7. **AUDITORIA**

5.17.7.1. A solução deve ser capaz de registrar todas as atividades realizadas, tanto de usuários quanto de administradores, gerando log com, no mínimo, as informações de data e hora, usuário, endereço de origem e informações completas das operações.

5.17.7.2. A solução deve registrar as falhas e exceções em log com informações suficientes para identificação da falha, com no mínimo as informações de data e hora, usuário, endereço de origem, informações completas das operações e depuração da falha ou exceção.

5.17.7.3. A solução deve manter o histórico de todas as informações geradas pela solução e que sofreram inclusões, alterações e exclusões por parte dos usuários da solução, pelo prazo definido pela CONTRATANTE.

5.17.7.4. A solução deve garantir que estes registros estejam protegidos contra alteração e exclusão.

5.17.7.5. A solução deve permitir a consulta e exportação das trilhas de auditoria, logs e históricos.

5.17.8. **COMPUTAÇÃO EM NUVEM**

5.17.8.1. Caso sejam utilizados recursos em nuvem, não serão permitidas conexões oriundas da internet para o ambiente da CONTRATANTE.

5.17.8.2. As informações disponibilizadas para nuvem serão somente aquelas exigidas para o funcionamento da solução.

5.17.8.3. A CONTRATADA deverá aferir mensalmente a disponibilidade da solução.

5.17.8.4. A CONTRATADA deverá disponibilizar documentação comprobatória da aferição da solução até o 5º (quinto) dia útil do mês subsequente à medição.

5.17.9. **RELATÓRIO GERENCIAL**

5.17.9.1. A solução deverá possuir relatório de utilização do múltiplo fator de autenticação.

5.17.9.2. A solução deverá permitir geração de relatório em ao menos um dos formatos: HTML, XML, DOCX, PDF ou CSV.

5.17.10. **HOMOLOGAÇÃO**

5.17.10.1. A homologação da integração da solução consiste na verificação do funcionamento completo da solução, respeitando os requisitos definidos neste documento.

5.17.10.2. A homologação da integração da solução deve ser realizada em conjunto entre a CONTRATADA e a CONTRATANTE, com a finalidade de homologar se todas as funcionalidades integradas e operacionais estão conforme as Especificações Técnicas.

5.17.10.3. Ao final da Integração e Homologação, a CONTRATANTE emitirá um Termo de Aceite Definitivo, que por sua vez não exime a CONTRATADA das responsabilidades do perfeito funcionamento da solução e da continuidade no atendimento a todos os requisitos constantes neste documento, no decorrer da vigência do contrato.

5.17.10.4. A instalação da solução em homologação deverá estar concluída no prazo de 30 (trinta) dias úteis, a partir da liberação do ambiente de homologação por parte da CONTRATANTE. Os itens considerados para

atendimento funcional da solução serão:

5.17.10.5. Comprovação da integração da solução com OWA e seu pleno funcionamento.

5.17.10.6. Comprovação da integração da solução com Palo Alto GlobalProtect, Fortinet FortiGate SSL VPN/FortiClient, VPN Cisco Anyconnect e seu pleno funcionamento.

5.17.10.7. Comprovação da integração da solução com VDI VMware Horizon 7 (ou superior) e seu pleno funcionamento.

5.17.10.8. Comprovação da integração da solução de RDP sem servidor gateway e seu pleno funcionamento.

5.17.10.9. Comprovação da integração da solução de RDP com servidor gateway e seu pleno funcionamento.

5.17.10.10. Comprovação da integração da solução com SSH e seu pleno funcionamento.

5.17.10.11. Comprovação da integração da solução com Microsoft Office 365 e seu pleno funcionamento.

5.17.10.12. Comprovação da integração da solução em logon nas estações de trabalho em ambiente interno da CONTRATANTE e seu pleno funcionamento.

5.17.10.13. Comprovação de que a solução gera relatórios, conforme Especificações Técnicas.

5.17.10.14. Para ser considerada apta, a CONTRATADA deverá, na homologação, demonstrar capacidade de atender a totalidade das Especificações Técnicas.

5.17.10.15. A CONTRATANTE ao final do processo de homologação emitirá relatório comprobatório de que todas as funcionalidades especificadas neste documento estão atendidas.

5.17.10.16. À CONTRATANTE caberá aceitar ou não a homologação, caso não seja aceito, a CONTRATADA deverá realizar os ajustes apontados pela CONTRATANTE.

5.18. Solução de firewall temporário

5.18.1. A CONTRATADA se compromete a instalar, em até 10 dias úteis após recebimento da Ordem de Fornecimento e em atendimento ao prazo descrito no item CONDIÇÕES DE ENTREGA, solução temporária de firewalls e gerência de firewalls virtualizados no Ambiente da PREFEITURA. A solução terá, no mínimo, a mesma capacidade, suporte e garantia que a solução física de firewalls, para garantir a continuidade dos serviços enquanto é aguardada a entrega, a instalação e migração dos Appliances definitivos.

5.18.2. Características da solução temporária de Firewalls virtualizada:

5.18.2.1. No mínimo 02 instâncias de firewalls e solução de Gerência, para que haja alta disponibilidade;

5.18.2.2. Possuir no mínimo de mesma capacidade de processamento que a solução de Appliances Físicos;

5.18.2.3. Ter as mesmas assinaturas de Subscrição de Próxima Geração (Filtro de URL avançado, Proteção Malware avançada e IPS de próxima geração) ativas por no mínimo o mesmo prazo descrito no item CONDIÇÕES DE ENTREGA.

5.18.3. A CONTRATADA deverá prover previamente a informação dos recursos de Hardware necessários à PREFEITURA para execução da solução de forma plena e garantir Alta disponibilidade do Serviço da Solução virtualizada de Firewalls.

5.18.4. A solução de Virtual Appliance, deve ser compatível com os seguintes Hypervisors:

5.18.4.1. Nutanix AHV versão AOS 5.20 e posterior;

5.18.4.2. Fornecer os arquivos de instalação ou de imagem (OVA ou similar) dos appliance virtuais, de maneira eletrônica;

5.18.4.3. Fornecer os arquivos ou chaves de licenças a serem instalados na solução. Também fornecer procedimento de transferência das licenças para outro equipamento (rehost) em caso de necessidade futura;

5.18.4.4. Deverá informar recursos de hardware adequados e conectividade recomendados para o pleno funcionamento da solução à PREFEITURA;

5.18.4.5. Ter o suporte das instâncias virtuais e gerência com validade durante o uso, com atendimento e suporte 24x7 inclusa;

5.18.4.6. A solução deve ser instalada dentro da PREFEITURA.

5.18.5. A CONTRATADA poderá fornecer, a critério da PREFEITURA, solução de appliances físicos temporários de modelo e marca idênticos ou superiores ao da solução final ofertada, bem como solução de gerência para os dispositivos do mesmo fabricante. A solução temporária (Firewall e Gerência de Firewalls) devem encontrar-se em linha produção (não estar descontinuados pelo Fabricante), apresentar desempenho igual ou superior aos Firewalls físicos solicitados pela PREFEITURA (inclusive com assinaturas de subscrição: Filtro de URL avançado, Proteção Malware avançada e IPS de próxima geração) durante o tempo de uso, além de suporte com atendimento 24x7x4 onsite incluso ativo durante o tempo de uso e a pronta entrega para instalação imediata, após recebimento da Ordem de Fornecimento.

5.19. **INSTALAÇÃO DAS SOLUÇÕES DE NEXT GENERATION FIREWALL, VPN E MÚLTIPLO FATOR DE AUTENTICAÇÃO.**

5.19.1. A CONTRATADA deverá atender aos seguintes requisitos para instalação e entrega do serviço:

5.19.1.1. Ter pelo menos um profissional certificado no nível “profissional” e/ou “expert” na solução, através de comprovação expedida pelo fabricante da solução;

5.19.1.2. Entregar atestados de capacidade técnica comprovando a instalação de solução igual ou semelhante.

5.19.2. O serviço de instalação e configuração compreende desde a configuração lógica, testes, até que a solução esteja ativa e em pleno funcionamento. Caberá a CONTRATADA realizar a instalação da solução nas dependências da PREFEITURA de acordo com a seguinte metodologia de trabalho:

5.19.2.1. Reunião preliminar com a equipe técnica da PREFEITURA para definir o escopo de serviços da instalação;

5.19.2.2. Elaboração e entrega de pré-projeto de instalação contendo as configurações principais a serem aplicadas e o cronograma de trabalho para aprovação da PREFEITURA;

5.19.2.3. Configuração preliminar dos produtos em ambiente de homologação;

5.19.2.4. Elaboração e entrega de relatório final contendo todos os aspectos da instalação realizada.

5.19.3. A execução dos serviços de instalação e configuração definidos para implantação do projeto deve contemplar um mínimo de 960 (novecentas e sessenta) horas comerciais, podendo ser distribuídas em horas locais na PREFEITURA ou remoto, e 32 (trinta e duas) horas fora do horário comercial;

5.19.4. Acompanhamento da instalação da solução (dentro das horas previstas).

5.19.5. O serviço deve incluir as seguintes atividades:

5.19.5.1. Planejamento;

5.19.5.2. Estudo, Criação/Migração de regras de firewall;

5.19.5.3. Criação de 2 (duas) DMZs;

5.19.5.4. Até 250 regras de entrada;

5.19.5.5. Até 250 regras de saída;

5.19.5.6. Configuração de novas regras de firewall (se aplicável);

5.19.5.7. Criação de rotas;

5.19.5.8. Criação de regras de QoS;

5.19.5.9. Criação e/ou comunicação com VLAN's;

5.19.5.10. Integração com serviços de rede;

5.19.5.11. Criação de regras de sistema de prevenção de intrusão (IPS);

5.19.5.12. Criação de regras de controle de aplicação;

5.19.5.13. Integração da solução com o Active Directory;

5.19.5.14. Instalação e configuração da Plataforma de Console;

5.19.5.15. Criação de novas regras de VPN;

5.19.5.16. Instalação de até 30 (trinta) VPNs, além de transferência de conhecimento e suporte para a equipe da PREFEITURA concluir a instalação dos clientes VPN restantes para os colaboradores da PREFEITURA;

5.19.5.17. Instalar até 30 (trinta) múltiplo fator de Autenticação para os usuários da PREFEITURA, contemplando:

5.19.5.17.1. Planejamento;

5.19.5.17.2. Configuração inicial da Solução SaaS do Fabricante;

5.19.5.17.3. Integração da solução com o Active Directory;

5.19.5.17.4. Integração da solução de MFA com até 20 (vinte) Aplicações;

5.19.5.17.5. Integração de até 20 usuários para a tecnologia de MFA com a solução de VPN.

5.19.5.18. Transferência de conhecimento de até 80 (oitenta) horas para os colaboradores da PREFEITURA.

## 5.20. MANUTENÇÃO E SUPORTE TÉCNICO

5.20.1. Todos os PRODUTOS fornecidos deverão possuir garantia de funcionamento, serviços de manutenção e suporte técnico, por um período de 48 (quarenta e oito) meses, a contar da data de emissão do termo de aceite dos produtos.

5.20.2. O serviço de manutenção deverá ser prestado nas dependências da PREFEITURA, exceto para as soluções de VPN e MFA.

5.20.3. O Serviço de manutenção e suporte técnico dos produtos deverão abranger a manutenção corretiva com cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a substituição de peças, partes, componentes e acessórios.

5.20.4. A modalidade de suporte a ser disponibilizado deverá ser 24x7x4, com substituição avançada de peças, sendo entregues dentro de quatro horas de determinação de que a peça a ser substituída é realmente necessária (24 horas por dia, 07 dias por semana), durante o horário normal de trabalho, sendo que todos os serviços onsite deverão ser de responsabilidade da CONTRATADA.

5.20.5. Com o objetivo de manter os equipamentos a serem fornecidos em boas condições de funcionamento ou restabelecê-lo a tais condições, a CONTRATADA prestará serviço de assistência técnica onsite durante o período de disponibilidade para as soluções, exceto as soluções de VPN e MFA.

5.20.6. O prazo para a CONTRATADA iniciar o atendimento via suporte técnico para diagnóstico do problema é de, no máximo, 30 (trinta) minutos, contado a partir da abertura do chamado e dentro do período de disponibilidade.

5.20.7. Proporcionar assistência técnica onsite comparecendo no prazo de até 04 (quatro) horas no local

(tempo de chegada), contado a partir da abertura do chamado e dentro do período de disponibilidade.

5.20.8. O prazo máximo de reparo e solução, contado a partir do chamado e dentro do período de disponibilidade é de 06 (seis) horas úteis, para os PRODUTOS fornecidos.

5.20.9. Para as soluções de Subscrição ou SaaS, o tempo de solução deverá ser de no máximo 06 (seis) horas. Caso haja eventual indisponibilidade acima do prazo de 06 (seis) horas, a CONTRATADA deverá apresentar todas as devidas justificativas do Fabricante à PREFEITURA, além de acompanhar a evolução da restauração completa do serviço, para que não ocorra penalidades.

5.20.10. A CONTRATADA deverá assegurar a assistência técnica necessária à satisfatória utilização dos equipamentos, no que consiste à manutenção de hardware, instalação, reinstalação e atualização de softwares/firmwares internos dos equipamentos.

5.20.11. Para prestação do serviço de garantia será exigido que a CONTRATADA habilite o suporte junto ao Fabricante, para todos os equipamentos relacionados

5.20.12. A CONTRATADA deverá disponibilizar para a PREFEITURA, durante o período de vigência da garantia, acesso automático às documentações e as versões de manutenção e atualizações de software/firmwares dos PRODUTOS, via portal web internet do fabricante, sob demanda, sem ônus à PREFEITURA.

5.20.13. A CONTRATADA deverá ter acesso direto ao suporte técnico especializado do Fabricante dos PRODUTOS, via telefone e e-mail, para solução dos problemas e encaminhamento dos problemas ao setor competente do Fabricante. Deve também disponibilizar uma senha de acesso para este serviço a equipe da PREFEITURA.

5.20.14. A CONTRATADA deverá disponibilizar número de telefone 0800, e-mail, além de sistema de abertura de chamados web à PREFEITURA.

5.20.15. A CONTRATADA acionará através de abertura e acompanhamento de chamados o centro de suporte técnico do Fabricante, bem como acompanhamento da resolução desses chamados e implantação das soluções sugeridas pelo Fabricante.

5.20.16. A assistência técnica da CONTRATADA deverá cobrir atendimento telefônico, sem limitação, durante a vigência do contrato.

5.20.17. A CONTRATADA prestará serviço de manutenção corretiva dos equipamentos no local de instalação dos mesmos, e será CONTRATADA pela entrega e instalação das peças de substituição, retirada das peças com defeitos e, se necessário, deverá efetuar a reconfiguração do sistema operacional dos equipamentos.

5.20.18. O Fornecimento e instalação de atualizações corretivas e evolutivas de programas (tais como firmware e sistema operacional dos produtos), necessárias ao bom funcionamento dos EQUIPAMENTOS.

5.20.19. A atividade de atualização de versões de Softwares operacionais dos EQUIPAMENTOS deve estar inclusa como um serviço de disponibilização e implantação de atualizações corretivas e evolutivas de versão, sem ônus adicional à PREFEITURA:

5.20.20. Qualquer atualização nos EQUIPAMENTOS somente será feita mediante conhecimento prévio da PREFEITURA;

5.20.21. Caso exista incompatibilidade e /ou insuficiência de algum componente de Hardware nos EQUIPAMENTOS para suportar uma eventual atualização de Sistema Operacional, caberá à CONTRATADA informar à PREFEITURA qual ou quais requisitos de Hardware devem ser atendidos. À PREFEITURA caberá

prover a adequação do Hardware necessária para suportar tal atualização, se esta for de interesse da PREFEITURA.

5.20.22. A CONTRATADA prestará os serviços de manutenção corretiva e suporte técnico nos EQUIPAMENTOS, independentemente dos acessórios ou outros equipamentos que estejam a este conectados.

5.20.23. A CONTRATADA prestará serviço de suporte técnico à configuração dos EQUIPAMENTOS que caracterizem a adequação da instalação ou melhoria no desempenho, em termos de segurança, produtividade, contingência ou outros benefícios. Isto poderá ocorrer por iniciativas de ambas as partes, sempre com anuência da PREFEITURA.

5.20.24. É facultado à PREFEITURA realizar a manutenção de primeiro nível nos EQUIPAMENTOS, provendo ajustes ou substituição das peças defeituosas, desde que executado por pessoal técnico devidamente treinado para realização dos serviços, não eximindo a CONTRATADA de quaisquer responsabilidades sobre o reparo dos EQUIPAMENTO.

5.20.25. A CONTRATADA deverá possuir número de telefone e fax com tarifação local da cidade de São Paulo ou serviço de Call Center 0800 (sem custo na ligação para a PREFEITURA) equivalente caso seja tarifação diferencial a localidade de São Paulo.

5.20.26. A CONTRATADA deverá possuir base de suporte ou equivalente num raio de até 100 km da sede da PREFEITURA para conseguir cumprir o atendimento dentro do prazo estabelecido.

## 6. SOLUÇÃO DE POLÍTICA DE SEGURANÇA E AUTENTICAÇÃO À REDE (NAC)

### 6.1. HARDWARE E SOFTWARE

6.1.1. A Solução de Autenticação, também conhecida como NAC (Network Admission Control), deverá ser instalada em servidor virtual na quantidade de no mínimo 02 (duas) instâncias virtuais, para que haja alta disponibilidade.

6.1.2. Tanto o hardware do servidor, bem como o sistema de virtualização não fazem parte do escopo.

6.1.3. O suporte das instâncias virtuais deve ser ter validade mínima de 48 (quarenta e oito) meses.

6.1.4. A CONTRATADA deverá prover previamente a informação dos recursos de Hardware necessários à PREFEITURA para execução da solução de forma plena e garantir Alta disponibilidade do Serviço da Solução de Política de Segurança e Autenticação.

6.1.5. A solução de Virtual Appliance, deve ser compatível com os seguintes Hypervisors:

6.1.6. Nutanix AHV versão AOS 5.20 e posterior;

6.1.7. VMware vSphere Hypervisor (ESXi) 6.5 ou superior.

6.1.8. Todo o licenciamento da solução deve ser entregue via subscrição com validade mínima de 05 (cinco) anos e suporte com atendimento 24x7 incluso.

6.1.9. Fornecer os arquivos de instalação ou de imagem (OVA ou similar), em caso de appliance virtual, de maneira eletrônica.

6.1.10. Fornecer os arquivos ou chaves de licenças a serem instalados na solução. Também fornecer procedimento de transferência das licenças para outro equipamento (rehost) em caso de necessidade futura.

6.1.11. Toda a solução deve ser instalada dentro da PREFEITURA.

6.1.12. São solicitados um total de 15.000 (quinze mil) licenças de endpoints como subscrição e suporte para

48 (quarenta e oito) meses para a Solução de Política de Segurança e Autenticação à rede pela PREFEITURA.

6.1.13. Do montante de licenças, serão 4.000 (quatro mil) licenças de endpoints deverão ser voltadas à Autenticação de ativos corporativos e BYOD na rede, realizar a classificação automática de ativos (ou visibilidade dos Ativos), além da segmentação baseada com base em grupos. Já 11.000 (onze mil) licenças de endpoints restantes serão utilizadas na autenticação de endpoints na rede visitantes (AAA, 802.1X e Acesso Guest) da rede da PREFEITURA.

6.1.14. A Solução de Autenticação deve ter capacidade para suportar no mínimo 25.000 (vinte e cinco mil) endpoints (dispositivos).

6.2. **CAPACIDADES E FUNCIONALIDADES**

6.2.1. Deve Integrar com switches, access points e controladoras de outros FABRICANTES por meio do protocolo RADIUS ou outros.

6.2.2. Informar aos sistemas externos, como firewalls de nova geração, o estado da sessão de cada dispositivo/usuário com todos os seus endereços IPs (IPv4 e IPv6) por meio de RADIUS Account, Syslog ou interface REST API. No mínimo o sistema deve informar o início de sessão, o fim de sessão e as trocas de endereço IP.

6.2.3. Deve possuir interface REST API que permita cadastro/remoção/bloqueio de dis-positivos/usuários em sua base local.

6.2.4. Permitir a alteração de autorização do dispositivo/usuário de forma imediata.

6.2.5. Deve possuir a funcionalidade de autenticação através de portal Web para usuários visitantes, temporários ou clientes corporativos, de forma integrada com as controladoras wireless. Estes usuários, uma vez autenticados, serão desviados para segmentos específicos da rede LAN (VLANs).

6.2.6. Esta funcionalidade deve ser independente da funcionalidade de autenticação através de portal Web para os usuários visitantes, temporários ou clientes corporativos, de forma integrada com a solução centralizada de autenticação para usuários. Estes usuários, uma vez autenticados, serão desviados para segmentos específicos da rede LAN (VLANs).

6.3. **AUTENTICAÇÃO DE USUÁRIOS E DISPOSITIVOS NA REDE.**

6.3.1. A solução deve implementar a autenticação de dispositivo e usuário na rede usando o protocolo IEEE 802.1X, suportando pelo menos os seguintes métodos EAP: EAP-MD5, EAP-TLS, PEAP, EAP-FAST e EAP-GTC

6.3.2. Deve implementar a autenticação do usuário / dispositivo usando as seguintes fontes de informações de identidade:

6.3.2.1. Interna, de usuário

6.3.2.2. Interna, de dispositivo

6.3.2.3. Com Autoridade Certificadora Interna

6.3.2.4. Externa via RADIUS

6.3.2.5. Externa via LDAP

6.3.2.6. Externa via SAMLv2 IdPs

6.3.2.7. Externa através do Windows Active Directory

6.3.2.8. Externa através de Autoridade de Certificação de Terceiros.

6.3.2.9. Externa via ODBC

6.3.2.10. Externa com servidores de Tokens

6.3.3. A solução deve oferecer autenticação de usuário através de um portal web HTTPS seguro com redirecionamento automático, tanto na rede sem fio quanto na rede com fio.

6.3.4. A solução deve implementar autenticação específica para dispositivos com base no endereço MAC.

6.3.5. A solução deve ter uma base de dados interna para registrar dispositivos pelo endereço MAC. Deve ser permitindo que tal base seja pré-preenchida automaticamente por meio de um mecanismo automático de detecção de perfil do dispositivo.

6.3.6. Deve a solução deve implementar a validação de certificados digitais com as seguintes características:

6.3.7. Suportar integração a uma CA externa (Autoridade Certificadora).

6.3.8. Suportar lista de revogação periódica CRL (Lista de revogação de certificados) via HTTP

6.3.9. Suportar o protocolo OCSP para verificação do status do certificado.

6.3.10. Possuir uma CA interna para dispositivos BYOD (Bring Your Own Device).

6.3.11. A solução deve implementar um mecanismo flexível de regras que permita selecionar o banco de dados onde um usuário e / ou dispositivo serão autenticados com base em atributos RADIUS existentes na solicitação enviada pelo equipamento de rede e tipo de protocolo, permitindo pelo menos o seguinte combinações de regras:

6.3.11.1. Com fio 802.1x

6.3.11.2. Wireless 802.1x

6.3.11.3. Autenticação sem 802.1x

6.3.12. O sistema deve poder obter informações de outros sistemas para realizar a identificação passiva de usuários, através de protocolos / especificações, como syslog e API REST.

6.3.13. O sistema deve poder fornecer informações para a identificação passiva de usuários em outros sistemas através de uma API.

6.3.14. Identificar e autenticar os dispositivos por certificado digital, credenciais de usuário/senha, MAC Address e Pre-Shared Key por usuário (senha de acesso a rede wireless única para cada dispositivo/usuário).

6.3.15. Permitir a validação das credenciais de usuário/senha por consulta ao Microsoft Active Directory, consulta à base de dados SQL (mínimo MySQL e MS SQL), consulta a serviços de autenticação do Facebook ou Google, consulta customizada a outros sistemas por meio de REST API e consulta a um servidor Radius externo.

6.3.16. Permitir a configuração do tempo máximo de sessão para reautenticação do dispositivo do cliente e identificação da VLAN que ele deve ser associado.

6.3.17. Permitir respostas/políticas de acesso customizadas por dispositivo/usuário ou grupo de dispositivos/usuários.

6.3.18. Permitir o agrupamento de dispositivos/usuários por grupos/OUs do Microsoft Active Directory, identificação de MAC address por fabricante (OUI), campo customi-zado de base de dados externa e grupo local da solução de autenticação

6.4. **AUTORIZAÇÃO**

6.4.1. Deve implementar a atribuição de VLAN pelo servidor de controle de acesso.

6.4.2. Deve implementar atribuição dinâmica de ACL

6.4.3. Deve implementar a atribuição ACL do tipo "filter-id"

6.4.4. Deve implementar a atribuição ACL "nomeada" compatível com controladores sem fio que a organização atualmente possui.

6.4.5. Deve implementar a atribuição ACL do tipo Redirecionamento da Web compatível com os switches e controladoras wireless Cisco da PREFEITURA.

6.4.6. Deve implementar o gerenciamento centralizado de ACLs com base em rótulos de grupo de segurança e monitoramento em tempo real do tráfego marcado.

6.4.7. Deve implementar o mapeamento de políticas MacSec de acordo com o padrão IEEE802.1AE

6.4.8. Deve implementar mapeamento de domínio de voz para telefones IP (domínio de voz).

6.4.9. Deve implementar a atribuição de parâmetros de re-autenticação 802.1X

6.4.10. Deve ter a funcionalidade de configurar dinamicamente as portas de acordo com o tipo de dispositivo detectado

6.4.11. Deve permitir a personalização de atributos de autorização

6.4.12. Deve permitir o agrupamento de atributos de autorização

6.4.13. Deve permitir a criação de perfis de usuários.

6.4.14. Deve suportar uma autorização de acesso condicional com base nos seguintes fatores:

6.4.14.1. Atributos LDAP do usuário autenticado;

6.4.14.2. Grupo de Active Directory (AD) do usuário autenticado;

6.4.14.3. Conteúdo do certificado digital (CN, OU);

6.4.14.4. Horário de conexões;

6.4.14.5. Meios de acesso;

6.4.14.6. Localização;

6.4.14.7. Tipo de dispositivo (exemplo: IPad, IPhone, Android, Windows, Mac OS);

6.4.14.8. Conformidade com as políticas de postura no Windows, Mac OS e sistemas móveis através da integração com sistemas MDM (Mobile Device Management);

6.4.14.9. Posicionamento físico de um dispositivo sem fio com base em uma área definida, via integração com um sistema de localização.

6.4.15. Deve suportar a combinação livre dos fatores descritos no item anterior.

6.4.16. Implementar o padrão RADIUS Change of Authorization (CoA).

6.4.17. Gestão de contas temporárias - Visitantes / Consultores:

6.4.17.1. Deve implementar um portal web SSL seguro para a criação de contas temporárias do tipo "visitante, consultor" com a autenticação de autorizadores baseados em Active Directory, LDAP e atribuição de privilégios para o autorizador de acordo com seu perfil.

6.4.17.2. Deve permitir a criação de perfis de contas temporárias, podendo atribuir diferentes privilégios de acesso à rede, contando com pelo menos os seguintes privilégios:

6.4.17.2.1. Perfil Visitante - Apenas acesso HTTP à Internet

6.4.17.2.2. Perfil Consultor - Apenas acesso HTTP à Internet e à Intranet

6.4.18. Deve permitir a criação de "Perfis de Tempo" estipulando, por exemplo, as seguintes opções de duração:

6.4.18.1. A conta temporária é válida por 1 dia a partir da sua criação.

6.4.18.2. A conta temporária é válida por 7 dias a partir da sua criação.

6.4.18.3. A conta temporária é válida por 1 dia a partir do primeiro login.

6.4.18.4. A conta temporária é válida por 7 dias a partir do primeiro login.

6.4.18.5. O autorizador determinará o início e o final de cada conta com base em seu privilégio de autorização

6.4.19. Deve permitir a criação de grupos de autorização com privilégios diferentes da criação de contas temporárias, especificando os seguintes privilégios por grupo:

6.4.19.1. Criar conta individual

6.4.19.2. Criar contas aleatórias

6.4.19.3. Importar contas de um arquivo .csv

6.4.19.4. Enviar credenciais por e-mail

6.4.19.5. Enviar credenciais via SMS

6.4.19.6. Ver a senha da conta do visitante

6.4.19.7. Imprimir os detalhes da conta do visitante

6.4.19.8. Visualizar e editar contas criadas por todos os grupos de autorizadores

6.4.19.9. Visualizar e editar contas criadas por autorizadores do mesmo grupo

6.4.19.10. Visualizar e editar as contas criadas pelo próprio autorizador

6.4.19.11. Suspender contas criadas por todos os grupos de autorizadores

6.4.19.12. Suspender contas criadas por autorizadores do mesmo grupo

6.4.19.13. Suspender contas criadas pelo próprio autorizador

6.4.19.14. Duração máxima da conta do visitante

6.4.19.15. Especificar o perfil de acesso à rede que será atribuído à conta do visitante

6.4.19.16. Especificar o perfil de tempo que será atribuído ao visitante

6.4.20. Deve permitir a personalização do formulário de criação de conta temporária que será completado pelo autorizador, especificando quais campos são necessários e quais são opcionais. A criação de novos campos personalizados também deve ser permitida. No entanto, o formulário a ser preenchido deve permitir que pelo menos os seguintes campos sejam especificados:

6.4.20.1. Nome;

6.4.20.2. Sobrenome;

6.4.20.3. Email;

6.4.20.4. Empresa ;

6.4.20.5. Telefone;

6.4.20.6. Campos personalizados.

6.4.21. Deve permitir a personalização do nível de segurança da senha temporária que será atribuída ao visitante, especificando o número mínimo de caracteres, o número de caracteres especiais e quantos números serão usados para compor a senha temporária.

6.4.22. Deve implementar um portal web seguro (HTTPS) que será automaticamente apresentado aos

usuários temporários (visitante / consultor) durante sua conexão com a rede (hotspot).

6.4.23. Deve permitir que a personalização das páginas do portal cativo (visitante / consultor) possa ser personalizada e a solução deve ser integrada a um editor gráfico exclusivo para este propósito, o que permitirá adicionar imagens de conteúdo, texto, botões e modificar o tema do portal (colunas, cores, etc.).

6.4.24. O layout dos portais deve ser adaptável ao tipo de dispositivo de usuário final, seja móvel ou desktop.

6.4.25. Deve ter suporte nativo para inglês, francês, italiano, espanhol, alemão, russo, chinês e português.

6.4.26. A CONTRATADA deve implementar autenticação via Web através de portal (Portal Captivo) para usuários visitantes e temporários, de forma integrada com o serviço de controladoras wireless. Estes usuários, uma vez autenticados, deverão ser desviados para segmentos específicos da rede LAN (VLANs). Esta implementação deve ser feita por meio de auto cadastro do usuário de suas credenciais (exemplo: nome, sobrenome, e-mail, telefone e demais informações relevantes);

6.4.27. O serviço web de autenticação (captive portal) deve ser fornecido e hospedado dentro da solução ofertada, além de permitir que as requisições possam ser redirecionadas para um serviço externo (internet).

6.4.28. A solução deve garantir a implementação de serviço de customização de no mínimo 03 (três) Portais de Autenticação (Captive Portal) funcionais para dispositivos móveis tais como computadores (laptops), tablets e celulares durante o contrato vigente. Este serviço poderá ser executado pela CONTRATADA através de Ferramenta da própria da Solução de Autenticação ou, na ausência de ferramenta, estes Portais serem impleementados pela equipe de Serviço Profissional do Fabricante (Advanced Services) para garantir a correta customização dos Portais de Autenticação, que inclui repasse de conhecimento a equipe da PREFEITURA. O portal deverá ser entregue com no mínimo:

6.4.28.1. Criação de Portal Guest - Hotspot e com credencial (Auto-registro ou com Patrocinador);

6.4.28.2. BYOD - Bring your own Device;

6.4.28.3. Ser totalmente integrado com a Plataforma de Política de Segurança e autenticação.

6.4.29. Deve ser capaz de implementar a opção "self-service" que permite que o usuário visitante crie sua própria conta temporária diretamente através do portal do hotspot seguro, sem a necessidade de um autorizador.

6.4.30. Deve implementar as seguintes funções no Portal da Web (hotspot).

6.4.30.1. Permitir a mudança de senha do usuário visitante diretamente no portal seguro;

6.4.30.2. Determinar o número máximo de dias antes de exigir uma alteração de senha;

6.4.30.3. Determinar o número máximo de erros de login antes de bloquear a conta;

6.4.30.4. Exigir a aceitação de "termos de uso aceitável da rede" em cada login na rede;

6.4.30.5. Exigir apenas no primeiro login a aceitação de "termos de uso aceitável de rede";

6.4.30.6. Personalização da página "Termos de uso aceitável da rede".

6.4.31. Deve ter uma API REST para poder fazer inscrições, alterações e exclusões de contas de convidados a partir de sistemas externos à solução (por exemplo, um sistema de controle de acesso físico);

6.4.32. Caso o gerenciador da Solução de Autenticação seja atendido totalmente ou parcialmente pela Solução Automação e Analytics, o fornecimento inicial deve somente incluir os itens complementares, como alguma ferramenta adicional e/ou licença;

6.4.33. Deve permitir através de interface gráfica a visualização e monitoramento dos autenticadores e dos dispositivos conectados à rede local, além da configuração dos equipamentos para aplicação de políticas de

segurança.

6.5. **CLASSIFICAÇÃO AUTOMÁTICA DE DISPOSITIVOS (PROFILING)**

6.5.1. Deve implementar mecanismo de detecção automática e transparente para dispositivos que se conectam à rede sem fio e com fio, classificando-os em uma das seguintes categorias:

6.5.1.1. Dispositivo Apple - Iphone, Ipad, Ipod, MAC;

6.5.1.2. Impressora - Lexmark, HP, Xerox;

6.5.1.3. Telefone IP - Cisco, Avaya;

6.5.1.4. Estação de trabalho - Windows, MAC OS;

6.5.1.5. Dispositivos IoT, como televisores, câmeras IP, projetores, sensores inteligentes.

6.5.2. Deve implementar os seguintes mecanismos para coletar informações de dispositivos, para serem usados na construção de regras de criação de perfil.

6.5.2.1. Coleta de tráfego DHCP e HTTP enviado pelo dispositivo;

6.5.2.2. Coleta de tráfego Netflow;

6.5.2.3. Coleta de atributos RADIUS relacionados à sessão 802.1X do dispositivo;

6.5.2.4. Consulta SNMP no switch de acesso ou na controladora wireless;

6.5.2.5. Consulta de DNS para resolução de nomes;

6.5.2.6. Iniciar a validação de portas TCP abertas no dispositivo;

6.5.2.7. Coleta de tráfego LLDP;

6.5.2.8. Coleta de informações do dispositivo no Active Directory.

6.5.3. Deve ter uma interface para a construção de regras personalizadas para a classificação do dispositivo, além de poder atribuir pesos e nível de certeza.

6.5.4. Deve permitir a criação de regras e categorias personalizadas.

6.5.5. Deve ter uma base de regras e categorias pré-configuradas.

6.5.6. Ele deve suportar um mecanismo para atualizar regras e categorias pré-configuradas.

6.5.7. Deve permitir que a classificação do dispositivo seja usada como parâmetro de autorização nas regras de acesso do dispositivo.

6.5.8. Deve permitir que o administrador registre manualmente um dispositivo específico em uma categoria

6.5.9. O sistema deve poder assinar e baixar automaticamente novas categorias e regras do site do fabricante.

6.6. **POSTURA DE ADMISSÃO (VERIFICAÇÃO)**

6.6.1. A solução deve suportar a verificação da postura das estações de usuários das seguintes maneiras:

6.6.1.1. Agente instalado: agente instalado na estação do usuário, responsável pela coleta de informações sobre a postura. O agente deve ser responsável apenas pela verificação da postura da estação. Todo o controle do nível de acesso à rede, controle de tempo concedido e controle de largura de banda deve ser realizado através do Sistema de Controle de Acesso.

6.6.1.2. Agente Temporário (no formato .exe ou .dmg): Agente que é carregado na estação no momento da verificação da postura para a coleta de informações sobre a postura. O agente deve ser responsável apenas pela verificação da postura da estação. Todo o controle do nível de acesso à rede, controle de tempo

concedido e controle de largura de banda deve ser feito através do Sistema de Controle de Acesso.

6.6.2. O Agente (Instalado ou Temporário) deve permitir a verificação dos seguintes itens:

6.6.2.1. Sistema operacional instalado;

6.6.2.2. Verificação do "Service Pack" instalado;

6.6.2.3. Chaves do Registro do Windows;

6.6.2.4. Arquivos existentes na estação do usuário;

6.6.2.5. Status dos serviços en execução na máquina;

6.6.2.6. Existência de Software Antivírus e AntiSpyware Instalado;

6.6.2.7. Data da última atualização do Antivírus;

6.6.2.8. Status do software Antivírus (ativado ou desativado);

6.6.2.9. Verificação de Hotfixes do Windows Instalados;

6.6.2.10. Inventário de aplicativos instalados;

6.6.2.11. Status de criptografia do disco rígido;

6.6.2.12. Portas USB.

6.6.3. A solução deve permitir a verificação da última versão dos Antivírus fornecidos. A solução deve ser capaz de verificar qual é a última assinatura disponível e a respectiva data. Os seguintes fabricantes de Antivírus devem ser suportados:

6.6.3.1. Symantec;

6.6.3.2. Trend Micro;

6.6.3.3. McAfee;

6.6.3.4. AVG;

6.6.3.5. Kaspersky;

6.6.3.6. Panda;

6.6.3.7. Sophos;

6.6.3.8. ClamAV;

6.6.3.9. Crowdstrike;

6.6.3.10. Cisco Secure Endpoint;

6.6.3.11. Avira.

6.6.4. A solução deve ter um banco de dados atualizado periodicamente com as informações de assinaturas de Antivírus, Anti-spyware e Hotfixes Microsoft.

6.6.5. O processo de verificação de postura, isolamento e remediação deve suportar um ambiente de telefonia IP, onde o equipamento informático está conectado à porta de rede do telefone IP e não diretamente ao switch. O fabricante é obrigado a esclarecer o design e os componentes necessários para conseguir isso.

6.7. **ISOLAMENTO E QUARENTENA**

6.7.1. O isolamento e a quarentena dos usuários devem ser orquestrados através do Sistema de Controle de Acesso.

6.7.2. A solução deve permitir isolamento de estações, mesmo que não tenham um agente instalado.

6.7.3. A solução deve permitir o isolamento de estações, mesmo que eles tenham um endereço IP

configurado estaticamente.

6.7.4. O isolamento deverá poder ser feito através de uma lista de acesso a ser baixada do Sistema de Controle de Acesso.

6.8. **REMEDIAÇÃO**

6.8.1. Caso o usuário não cumpra os requisitos de segurança da estação, a solução deve ter suporte a mecanismos de atualização das seguintes maneiras:

6.8.1.1. Manual: o agente instalado deve orientar o usuário no processo de atualização da estação (fornecendo hiperlinks para os patches, atualização de software Antivírus, atualizações do WSUS) para que a estação atenda as políticas de segurança.

6.8.1.2. Automático: o agente instalado deve executar o processo inteiro automaticamente.

6.8.2. A solução deve suportar a configuração das seguintes formas de remediação:

6.8.2.1. Distribuição de links Web;

6.8.2.2. Distribuição de arquivos;

6.8.2.3. Integração com WSUS e SCCM;

6.8.2.4. Integração com Antivírus e Antispyware.

6.8.3. A solução deve fornecer integração com o servidor WSUS para a instalação de patches de segurança do Windows. O agente instalado deve se comunicar com o WUA (Windows Update Agent) para verificar se há uma atualização pendente. Se for necessária qualquer atualização, o agente instalado deve iniciar uma atualização usando WUA de acordo com o mecanismo de atualização configurado (Manual ou Automático). Esta atualização deve ser transparente para o usuário e usar as APIs presentes no agente WUA.

6.8.4. A solução deve fornecer integração com os softwares Antivírus e Anti-spyware listados nesta especificação. Se for necessária qualquer atualização, o agente instalado deve iniciar uma atualização dos softwares Antivírus e Antispyware de acordo com o mecanismo de atualização configurado (Manual ou Automático). Esta atualização deve ser transparente para o usuário e usar as APIs presentes nos softwares Antivírus e Antispyware.

6.9. **CONTROLE DE DISPOSITIVOS PESSOAIS E "BYOD (BRING YOUR OWN DEVICE)"**

6.9.1. A solução deve implementar a criação de regras para a diferenciação de dispositivos corporativos e pessoais, possibilitando a adoção de políticas de "BYOD (Bring Your Own Device)":

6.9.1.1. Deve fornecer um portal para os usuários registrarem e gerenciarem seus próprios dispositivos para uso na rede.

6.9.1.2. Deve permitir a integração com sistemas MDM (Mobile Device Management)

6.9.1.3. Deverá possuir uma Autoridade Certificadora interna para o aprovisionamento e gerenciamento de certificados digitais para dispositivos BYOD.

6.9.1.4. auto-registro de dispositivos dos usuários deve suportar o aprovisionamento de um certificado digital que identifique o dispositivo BYOD e sirva como um método de autenticação para a rede com fio e sem fio.

6.9.1.5. O administrador deverá ter a capacidade de suspender/reativar dispositivos e revogar certificados a partir da interface de gerência da solução.

6.10. **GERENCIAMENTO DE EQUIPAMENTOS DE REDE**

6.10.1. A solução deve ser capaz de gerenciar autenticação, autorização e contabilidade em dispositivos de rede, tais como switches, roteadores, firewalls e equipamentos de rede WLAN por meio do protocolo TACACS+ padrão.

6.10.2. O gerenciamento de AAA por meio do TACACS+ deve permitir a autorização granular dos comandos que um administrador de rede pode executar em um equipamento de rede configurado com este protocolo.

6.10.3. Deve ter perfis de autorização de comandos predefinidos (out-of-the-box) para o gerenciamento de controladoras WLAN, roteadores e switches, de tal forma que não seja necessário criar listas de comandos a partir do zero.

6.10.4. Deve ser possível gerar logs para auditorias de autenticações, autorizações e comandos executados nos dispositivos de rede configurados com TACACS+.

6.10.5. Deve suportar a função de proxy do protocolo TACACS+.

6.10.6. Deve suportar TACACS+ sobre IPv6.

6.11. **GESTÃO E ADMINISTRAÇÃO DA POLÍTICA DE SEGURANÇA**

6.11.1. A solução deve ser capaz de gerenciar, configurar e modificar regras e políticas através de uma interface gráfica na web, acessível por HTTPS.

6.11.2. Deve ter um Painel (Dashboard) para visualização rápida das seguintes informações resumidas:

6.11.2.1. Métricas das últimas 24 horas;

6.11.2.2. Número de dispositivos ativos;

6.11.2.3. Número de visitantes ativos;

6.11.2.4. Tempo médio para remediação do dispositivo;

6.11.2.5. Porcentagem de dispositivos que atendem a postura;

6.11.2.6. Número de dispositivos classificados (profiling);

6.11.2.7. Informação de desempenho, CPU, Memória de cada componente da solução;

6.11.2.8. Número total de falhas de autenticação nas últimas 24 horas e o motivo principal;

6.11.2.9. Deve ter uma tela de monitoramento contínuo de autenticações em tempo real com visualização imediata das seguintes informações:

6.11.2.9.1. Data e hora;

6.11.2.9.2. Capacidade de visualização avançada (Drill-down) para detalhamento de autenticação e autorização;

6.11.2.9.3. Status de autenticação;

6.11.2.9.4. Nome de usuário / dispositivo;

6.11.2.9.5. Endereço MAC;

6.11.2.9.6. Endereço IP;

6.11.2.9.7. Equipamento de rede em que se deu a conexão;

6.11.2.9.8. Interface de rede em que se deu a conexão;

6.11.2.9.9. Perfil de autorização atribuído;

6.11.2.9.10. Resultado de classificação do dispositivo – Categoria;

6.11.2.9.11. Status de postura (conformidade);

6.11.2.9.12. Razão em caso de falha;

6.11.2.9.13. Método de autenticação;

6.11.2.9.14. Protocolo de Autenticação.

6.11.3. Deve ser capaz de gerar relatórios com informações sobre o resultado da verificação da postura da máquina.

6.12. **CAPACIDADE E INTEGRAÇÃO**

6.12.1. Deve suportar um mecanismo de alta disponibilidade para todas as funções do Sistema de Controle de Acesso;

6.12.2. Em caso de falha em qualquer appliance (físico ou virtual), nenhuma intervenção manual será necessária para recuperar ou executar failover;

6.12.3. A solução deve suportar uma arquitetura totalmente centralizada de seus serviços, ou seja, sem a necessidade de implementar appliances fora do Data Center e suportando todas as funcionalidades indicadas nas seções anteriores;

6.12.4. A solução deve suportar a operação em appliances de hardware de propósito específico.

6.12.5. No caso de uma implementação de appliance de hardware de propósito específico, deve ter a capacidade de vincular as interfaces de rede;

6.12.6. A API para integração com terceiros deve basear-se em padrões e arquitetura descentralizada cliente-servidor, de tal forma que as integrações não serão 1-a-1 para cada novo sistema que seja adicionado;

6.12.7. Para proteger o investimento e evitar custos subsequentes que não foram contemplados dentro deste projeto, será dada preferência aos sistemas que não exigem licenciamento adicional para cada integração com terceiros;

6.12.8. Suporte para o protocolo de autenticação extensível de túnel (TEAP);

6.12.9. Permitir através do encadeamento EAP executar os métodos internos para autenticação do usuário e da máquina dentro do mesmo túnel TEAP;

6.12.10. A ferramenta de Autenticação suportar integração com solução de proteção de cargas de trabalho, bem como enviar contextos de usuários, postura do dispositivo terminal e outras informações do terminal para a Plataforma de CWPP, tais como Cisco Secure Workload ou Guardicore ou Illumio;

6.12.11. Suportar correlacionamento os resultados da autenticação e aplique a política de autorização apropriada, usando o atributo EAPChainingResult;

6.12.12. A solução dispõe um gateway de API de gerenciamento, que atua como um único ponto de entrada para várias APIs de serviço para fornecer melhor segurança e gerenciamento de tráfego;

6.12.13. A solução de NAC deve possuir ainda plataforma dedicada com a finalidade de integração que permite que vários produtos de Segurança compartilhem dados [CONTEXTOS]. A plataforma deve:

6.12.13.1. Ser aberta, escalonável e baseada nos padrões IETF para ajudar a Automatizar a Segurança para obter respostas e conter ameaças com maior rapidez;

6.12.13.2. Por meio da Plataforma devem ser aplicadas Políticas de Segurança dinâmicas na rede com base nas requisições vindas das Soluções de Parceiros de Segurança, trocando Contextos, por exemplo, entre as Ferramentas de Gestão de Vulnerabilidades, Proteção a Carga de Trabalho e a solução de NAC.

6.12.14. A solução permite a assinatura de certificados por Impressão Digital (Certificate Fingerprinting);

6.12.15. A solução tem opção de verificação de integridade é introduzida para diagnosticar todos os nós em

sua implantação, chamados de Health Checks;

6.12.16. Permitir executar autorização e autenticação em uma rede com provedores de identidade baseados em nuvem;

6.12.17. A solução deve permitir a funcionalidade MS-Eventing API ou Microsoft Remote Procedure Call (MSRPC) protocol para Passive Identity;

6.12.18. A solução permite a criação uma política de postura para definir uma versão mínima de antivírus e antimalware para os endpoints em sua rede.

6.12.19. A solução deve ter a opção de Agentless Posture - esse novo tipo de postura entrega um agente ao cliente por meio de SSH e, opcionalmente, remove o cliente quando a postura é concluída.

6.13. **INSTALAÇÃO DA SOLUÇÃO DE POLÍTICA DE SEGURANÇA E AUTENTICAÇÃO À REDE (NAC)**

6.13.1. A CONTRATADA deverá atender aos seguintes requisitos para instalação e entrega do serviço:

6.13.2. Ter pelo menos um profissional certificado no nível “profissional” e/ou “expert” na solução, através de comprovação expedida pelo fabricante da solução;

6.13.3. Entregar atestados de capacidade técnica comprovando a instalação de solução igual ou semelhante.

6.13.4. O serviço de instalação e configuração compreende desde a configuração lógica, testes, até que a solução esteja ativa e em pleno funcionamento. Caberá a CONTRATADA realizar a instalação da solução nas dependências da PREFEITURA de acordo com a seguinte metodologia de trabalho:

6.13.5. Reunião preliminar com a equipe técnica da PREFEITURA para definir o escopo de serviços da instalação;

6.13.6. Elaboração e entrega de pré-projeto de instalação contendo as configurações principais a serem aplicadas e o cronograma de trabalho para aprovação da PREFEITURA;

6.13.7. Configuração preliminar dos produtos em ambiente de homologação;

6.13.8. Elaboração e entrega de relatório final contendo todos os aspectos da instalação realizada.

6.13.9. A execução dos serviços de instalação e configuração definidos para implantação do projeto deve contemplar um mínimo de 700 (setecentas) horas comerciais, podendo ser distribuídas em horas locais na PREFEITURA ou remoto, além de 116 (cento e dezesseis) horas fora do horário comercial;

6.13.10. Acompanhamento da instalação da solução (dentro das quarenta horas prevista).

6.13.11. O serviço inclui as seguintes configurações:

6.13.11.1. Planejamento e Design;

6.13.11.2. Instalação da solução virtualizada de NAC;

6.13.11.3. Aplicação das políticas e configurações de 802.1x nos Switches da PREFEITURA;

6.13.11.4. Integração da Solução com Active Directory;

6.13.11.5. Configurações de Autenticação e Postura;

6.13.11.6. Configurações de políticas GUEST;

6.13.11.7. Confecção, configuração e integração de 03 (três) portais (splash page) com a Solução de NAC;

6.13.11.8. Configuração da funcionalidade TACACS;

6.13.11.9. Operação Assistida;

6.13.11.10. Documentação Geral.

6.13.12. Transferência de conhecimento de até 32 (oitenta) horas para os colaboradores da PREFEITURA.

6.14. **MANUTENÇÃO E SUPORTE TÉCNICO**

6.14.1. A solução fornecida deverá possuir garantia de funcionamento, serviços de manutenção e suporte técnico, por um período de 48 (quarenta e oito) meses, a contar da data de emissão do termo de aceite do produto.

6.14.2. O Serviço de manutenção e suporte técnico deverá abranger a manutenção corretiva com cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a substituição de peças, partes, componentes e acessórios.

6.14.3. A modalidade de suporte a ser disponibilizado deverá ser 24x7 (24 horas por dia, 07 dias por semana) de responsabilidade da CONTRATADA.

6.14.4. Caso haja eventual indisponibilidade nas Soluções de Subscrição ou SaaS e esta indisponibilidade superar o prazo de 06 (seis) horas, a CONTRATADA deverá apresentar todas as devidas justificativas do Fabricante à PREFEITURA, além de acompanhar a evolução da restauração completa do serviço, para que não ocorra penalidades.

6.14.5. A CONTRATADA deverá assegurar a assistência técnica necessária e satisfatória das soluções, no que consiste à manutenção, reinstalação e atualização de softwares/firmwares das soluções.

6.14.6. Para prestação do serviço de garantia será exigido que a CONTRATADA habilite o suporte junto ao Fabricante, para todos as soluções relacionadas

6.14.7. A CONTRATADA deverá disponibilizar para a PREFEITURA, durante o período de vigência da garantia, acesso automático às documentações e as versões de manutenção e atualizações de software/firmwares dos PRODUTOS, via portal web internet do fabricante, sob demanda, sem ônus à PREFEITURA.

6.14.8. A CONTRATADA deverá ter acesso direto ao suporte técnico especializado do Fabricante dos PRODUTOS, via telefone e e-mail, para solução dos problemas e encaminhamento dos problemas ao setor competente do Fabricante. Deve também disponibilizar uma senha de acesso para este serviço a equipe da PREFEITURA.

6.14.9. A CONTRATADA acionará através de abertura e acompanhamento de chamados o centro de suporte técnico do Fabricante, bem como acompanhamento da resolução desses chamados e implantação das soluções sugeridas pelo Fabricante.

6.14.10. A assistência técnica da CONTRATADA deverá cobrir atendimento telefônico, sem limitação, durante a vigência do contrato.

6.14.11. O Fornecimento e instalação de atualizações corretivas e evolutivas de programas (tais como firmware e sistema operacional dos produtos), sempre que solicitadas pela PREFEITURA, necessárias ao bom funcionamento das soluções.

6.14.12. Qualquer atualização nos EQUIPAMENTOS somente será feita mediante conhecimento prévio da PREFEITURA;

6.14.13. A CONTRATADA prestará os serviços de manutenção corretiva e suporte técnico das soluções contratadas, independentemente dos acessórios ou outros equipamentos que estejam a este conectados.

6.14.14. É facultado à PREFEITURA realizar a manutenção de primeiro nível nas soluções, desde que executado por pessoal técnico devidamente treinado para realização dos serviços, não eximindo a

CONTRATADA de quaisquer responsabilidades sobre o reparo nas soluções.

6.14.15. A CONTRATADA deverá disponibilizar número de telefone 0800, e-mail, além de sistema de abertura de chamados web à PREFEITURA.

6.14.16. A CONTRATADA deverá possuir número de telefone e fax com tarifação local da cidade de São Paulo ou serviço de Call Center 0800 (sem custo na ligação para a PREFEITURA) equivalente caso seja tarifação diferencial a localidade de São Paulo.

6.14.17. A CONTRATADA deverá possuir base de suporte ou equivalente num raio de até 100 km da sede da PREFEITURA para conseguir cumprir o atendimento dentro do prazo estabelecido.

## 7. SOLUÇÃO DE PROTEÇÃO DE DNS RECURSIVO

### 7.1. CARACTERÍSTICAS GERAIS

7.1.1. A solução deve trazer última camada de proteção, trazendo rápido benefício aos usuários e colaboradores da PREFEITURA ao validar o acesso a internet por meio de DNS´s válidos.

7.1.2. Parametrizar a solução de proteção de redes baseada em segurança de DNS, de acordo com as orientações e padrões de Segurança da Informação da PREFEITURA.

7.1.3. Configurar e validar as regras de proteção de redes baseada em segurança de DNS na solução usada pela PREFEITURA, habilitando o bloqueio automático dos acessos indevidos ou maliciosos para os sistemas que se encontram em modo de aprendizado.

7.1.4. Operar a solução de proteção de redes baseada em segurança de DNS de acordo com as solicitações da PREFEITURA.

7.1.5. Configurar, verificar e validar o envio automático dos alertas de segurança da informação emitidos pela solução de proteção de redes baseada em segurança de DNS para as ferramentas de correlação de incidentes de segurança da informação da PREFEITURA.

### 7.2. HARDWARE E SOFTWARE

7.2.1. A Solução deve ser entregue com licenças como subscrição, no modelo de Software como Serviço em nuvem (SaaS).

7.2.2. A Solução de proteção de DNS recursivo deverá ser instalada em servidores virtualizados a quantidade de no mínimo 02 (duas) instâncias virtuais distintas, para que haja alta disponibilidade.

7.2.3. Tanto o hardware do servidor, bem como o sistema de virtualização não fazem parte do escopo.

7.2.4. O suporte das instâncias virtuais deve ser ter validade mínima de 48 (quarenta e oito) meses.

7.2.5. A CONTRATADA deverá informar previamente os recursos de Hardware necessários à PREFEITURA para execução da solução de forma plena e garantir Alta disponibilidade do Serviço da Solução de Política de Segurança e Autenticação.

7.2.6. A solução de Appliance virtual de proteção de DNS recursivo deverá ser compatível com os seguintes Hypervisors:

7.2.6.1. Nutanix AHV versão AOS 5.20 e posterior;

7.2.6.2. VMware vSphere Hypervisor (ESXi) 6.5 ou superior.

7.2.7. Deve ser entregue com capacidade para no mínimo 15000 (quinze mil) licenças, sendo 2500 para colaboradores e 12500 licenças de proteção de DNS recursivo para alunos.

7.2.8. Todo o licenciamento da solução deve ser entregue via subscrição com validade mínima de 48 (quarenta) meses e suporte com atendimento 24x7 incluso.

7.2.9. A CONTRATADA deve fornecer os arquivos de instalação ou de imagem (OVA ou similar), em caso de appliance virtual, de maneira eletrônica, além dos arquivos ou chaves de licenças a serem instalados na solução. Também fornecer procedimento de transferência das licenças para outro equipamento (rehost) em caso de necessidade futura.

7.3. **CARACTERÍSTICAS DO SERVIÇO DE DNS RECURSIVO**

7.3.1. **CONDIÇÕES GERAIS**

7.3.2. A solução deve ser efetiva e permanecer ativa em todo momento, independentemente da conectividade do cliente.

7.3.3. Dever causar impacto mínimo de performance para o usuário e no endpoint.

7.3.4. Deve possuir infraestrutura de resolução de nomes (filtro DNS) em Datacenter localizado no território brasileiro, sendo permitida a replicação desta infraestrutura em outras localidades;

7.3.5. Deve operar nativamente e permitir o uso de uma política geral de segurança na camada DNS.

7.3.6. Deve integrar de forma simples no sistema de DNS atual do ambiente de produção, especificamente substituindo as referências de servidores recursivos externos em uso.

7.3.7. As capacidades de segurança da solução não devem introduzir alta latência nas pesquisas durante a resolução DNS.

7.3.8. Deve permitir proteger todas as plataformas cliente e servidor do ambiente que utilizem comunicação internet através de resolução DNS.

7.3.9. A solução deve possuir capacidade inteligente de realizar inspeção pontual de páginas web suspeitas através da identificação de um domínio.

7.3.10. Deve possuir base de usuários protegidos no Brasil de, no mínimo, 60.000 (sessenta mil) usuários.

7.3.11. Deve possuir base de usuários protegidos no exterior (fora do Brasil) de, no mínimo, 60.000 (sessenta mil) usuários. Estes pontos acima podem ser comprovados através de documentação pública do fabricante ou atestados de capacidade técnica emitidos por clientes.

7.3.12. A solução deve possuir suporte para expansão de módulo Secure Web Gateway, ou seja, realizar inspeção não somente na camada do protocolo DNS, mas também aprofundar e avaliar a camada de protocolo HTTP/HTTPS

7.3.13. Deve imediatamente reduzir a quantidade de recursos usados para obter visibilidade, prevenção e contenção de infecções malware no ambiente local e usuários remotos.

7.3.14. Deve implementar a prevenção (bloqueio) de malwares avançados em diversos vetores de ataque.

7.3.15. Deve bloquear tráfego de Comando e Controle (C&C, C2, CallBack, PhoneHome) para evitar exfiltração de dados e outros mecanismos de controle remoto implementados por malwares e botnets.

7.3.16. Deve utilizar tecnologia que implementa diversos métodos de descoberta e inteligência de ameaças proprietária.

7.3.17. Deve realizar a detecção e prevenção de DGA's (domain generation algorithm) em tempo real, permitindo a obtenção de inteligência e elementos de correlação com outras infraestruturas globais em uso no contexto observado.

7.3.18. Deve permitir o uso de API programável e documentada para consulta, integração e complemento de inteligência de ameaças com sistemas externos.

7.3.19. Não deve conflitar com nenhum sistema anti-vírus local.

7.3.20. O mecanismo de proteção proativo e automático atuante na monitoração em tempo-real da solução durante as pesquisas DNS não pode ser um elemento tipo add-on, ou seja, deve ser uma funcionalidade núcleo da solução, que não dependa de repasse de ações de bloqueio para sistemas externos firewall, IPS ou proxy no controle de acesso.

7.3.21. A solução deve incorporar a capacidade de controle de acesso por categorias implementado em nível DNS mesmo quando não relacionadas a segurança.

7.3.22. Deve permitir a definição de listas personalizadas de acesso, para permitir (whitelisting) e para bloqueio (blacklisting) incluindo a capacidade de fazer o upload destas.

7.3.23. A solução deve permitir o controle de acesso baseado em políticas que incorporem identidades como elementos de decisão de contexto de acesso, incluindo os decorrentes de capacidade de integração com Microsoft Active Directory como:

7.3.23.1. Usuários;

7.3.23.2. Grupos;

7.3.23.3. Sistemas/endpoints;

7.3.23.4. Redes, IP's, CIDR.

7.3.24. A solução não deve depender de listas locais, feeds, antivirus ou proxies para:

7.3.24.1. A manutenção e automação do conteúdo das categorias de segurança padrão.

7.3.24.2. Considerar a visibilidade e detecção de condições de fast fluxing de infraestruturas e domínios suspeitos, maliciosos e dinâmicos;

7.3.24.3. Considerar a visibilidade e prevenção de exposição a condições como ataques incorporando domain-shadowing e cadeias acesso a gates e portais de distribuição de malwares e ataques.

7.3.25. Deve permitir estabelecer configurações que viabilizem a monitoração, prevenção e controle em redes remotas onde o endereçamento internet mude em intervalos de tempo (dinâmico).

7.3.26. Deve permitir a monitoração e prevenção em nível DNS para usuários for a da rede da empresa, utilizando para isto o mesmo serviço.

7.3.27. Deve permitir a personalização de múltiplas páginas de bloqueio de acesso e uso em distintas políticas de forma simultânea.

7.3.28. Deve permitir que condições de bloqueio sejam tratadas de forma diferente, incluindo recursos de bypass configurável por usuários e códigos com tempo de duração pré-estabelecidos para contextos específicos de acesso e categorias.

7.3.29. Deve permitir a delegação de acessos e permissões para administração de forma específica facilitando a tomada de decisão durante o gerenciamento de incidentes.

7.3.30. Deve permitir a definição de critérios de integração com plataformas terceiras de forma específica pela interface de gerenciamento.

7.3.31. Deve permitir configuração de mecanismo SAML (Security Assertion Markup Language) para autenticação, como okta, pingID, onelogin e outros por definição de metadata.

7.3.32. Deve permitir a utilização de mecanismo para implementar dois fatores de autenticação para acesso a

console de gerenciamento, permitindo o uso de google authenticator.

7.3.33. Não deve conflitar com nenhum sistema sandbox posicionado como endpoint em segmentos de rede ou plataforma gateway.

7.3.34. Não deve precisar de um mecanismo firewall para bloqueio de exposição a ameaças em tempo-real.

7.3.35. A solução deve suportar funcionalidade de segurança que protege os colaboradores mesmo que atuaem fora das dependências da PREFEITURA ou quando estiverem com a VPN desativada, permitindo proteção contínua contra malware, phishing e retornos de chamadas de comando e controle aonde quer que os usuários estejam.

7.3.36. Não deve precisar realizar nenhum tipo de inspeção profunda no tráfego internet para permitir o bloqueio de acesso a infraestruturas dinâmicas suspeitas, realizando a distribuição de ameaças ou comprometidas em tempo-real.

7.3.37. Não deve precisar de integração com Proxy para bloqueio de ameaças em tempo-real.

7.3.38. Deve possuir a capacidade de estabelecer reputação, tagging e inteligência de domínios por mecanismos predictivos e dinâmicos, utilização de modelagem estatística e aproveitamento automático de utilização de domínios globalmente.

7.3.39. Deve permitir o aproveitamento de visibilidade automática de comportamento e inteligência BGP ao intercambiar dados de rotas DNS com internet exchange providers em escala global.

7.3.40. Não deve ser uma solução para configuração, manutenção, implementação e serviço de DNS autoritativo.

7.3.41. Suportar a utilização do mesmo cliente VPN instalado nas máquinas de colaboradores da PREFEITURA, evitando assim conflitos de uso entre as aplicações.

7.3.42. Não deve ser uma solução para substituição de infraestrutura DNS interno, serviço DHCP ou firewall.

7.3.43. Deve nativamente permitir estabelecer detecção, reputação e inteligência de infraestruturas e domínios por modelos automáticos de co-ocorrência em escala global (concorrência de acessos).

7.3.44. Deve nativamente permitir estabelecer detecção, reputação e inteligência de infraestruturas pela monitoração automática de endereçamento IP e suas respectivas ASN incluindo atribuição DNS e correlação WHOIS automática.

7.3.45. Deve nativamente e automaticamente permitir a monitoração através de uma modelagem continua que quantifica, estabelece ranking e percebe padrões de utilização de infraestruturas, estabelecendo critérios de detecção e correlação com campanhas e mecanismos direcionados de ataques.

7.3.46. A solução deve possuir mecanismos automáticos de roteamento por anycast em escala global.

7.3.47. A solução deve permitir páginas de bloqueio customizáveis, configuração de bypass ou sinkhole.

7.3.48. Deve permitir um mecanismo de busca de inteligência para domínios, IP’s, HASH, incluindo a automação destas por uso de API’s.

7.3.49. Não seram aceitas soluções IPAM (IP address management).

7.3.50. Deve permitir implementar um mecanismo de integração com SPLUNK.

7.3.51. A solução deve nativamente estar preparada para utilização com serviço amazon S3 bucket.

7.3.52. Deve permitir proteger sistemas dentro e fora do perímetro de segurança.

7.3.53. Deve ser capaz de alimentar inteligência de ameaças a plataformas SIEM (Security Information and Event Management).

7.3.54. Solução deve possuir integração nativa com solução SOAR para criação de processos automatizados de investigação e otimização do tempo de resposta à incidentes.

7.3.55. Deve ser capaz de monitorar a utilização de serviços em nuvem (Cloud Services) para identificar riscos e desenvolver atividades de conformidade de forma automática.

7.3.56. Deve permitir a identificação de ataques direcionados.

7.3.57. Deve entregar relatórios, filtros e capacidade de análise de eventos a partir dos mesmos.

7.3.58. Deve permitir a comparação do tráfego DNS local e utilização de um domínio contra os padrões globais de tráfego.

7.3.59. Solução deve possuir mecanismo nativo de pesquisa de domínio, sendo capaz de fornecer informações sobre histórico de mudanças do estado do domínio, registro, malware associado (se existente) e uma avaliação de risco do domínio baseado em uma escala (1-10 ou 1-100, por exemplo).

7.3.60. Deve permitir a visualização de informações além de endereços IP ou DNS como o relacionamento inteiro com a ASN (autonomous system number).

7.3.61. Deve permitir exportar logs DNS para um repositório terceiro para análise posterior.

7.3.62. Deve possuir inteligência de ameaças atualizada de forma contínua em escala global (Internet) e customizada, criando assim um mecanismo dinâmico de reputação além de recursos padronizados de forma estática.

7.3.63. Deve nativamente permitir o uso de inteligência gerada por tecnologia de virtualização de artefatos sejam suspeitos ou maliciosos, incorporando diretamente no processo de defesa proativa em nível DNS de forma automática.

## 7.4. SERVIÇO INSTALAÇÃO DA SOLUÇÃO DE PROTEÇÃO DE DNS RECURSIVO

7.4.1. A CONTRATADA deverá atender aos seguintes requisitos para instalação e entrega do serviço:

7.4.1.1. Ter pelo menos um profissional certificado no nível “profissional” e/ou “expert” na solução, através de comprovação expedida pelo fabricante da solução;

7.4.1.2. Entregar atestados de capacidade técnica comprovando a instalação de solução igual ou semelhante.

7.4.2. O serviço de instalação e configuração compreende desde a configuração lógica, testes, até que a solução esteja ativa e em pleno funcionamento. Caberá a CONTRATADA realizar a instalação da solução nas dependências da PREFEITURA de acordo com a seguinte metodologia de trabalho:

7.4.2.1. Reunião preliminar com a equipe técnica da PREFEITURA para definir o escopo de serviços da instalação;

7.4.2.2. Elaboração e entrega de pré-projeto de instalação contendo as configurações principais a serem aplicadas e o cronograma de trabalho para aprovação da PREFEITURA;

7.4.3. A execução dos serviços de instalação e configuração definidos para implantação do projeto deve contemplar um mínimo de 300 (trezentas) horas comerciais, podendo ser distribuídas em horas locais na PREFEITURA ou remoto, e 32 (trinta e duas) horas fora do horário comercial;

7.4.4. Acompanhamento da instalação da solução (dentro das quarenta horas prevista).

7.4.5. O serviço inclui as seguintes configurações:

7.4.5.1. Planejamento;

7.4.5.2. Acompanhamento do provisionamento da Solução SaaS no Fabricante;

7.4.5.3. Instalação de Máquina virtual da solução de Proteção de DNS recursivo;

7.4.5.4. Integração com o Active Directory;

7.4.5.5. Realizar as configuração das políticas;

7.4.5.6. Janela de manutenção para a implementação da solução, com instalação de Agentes para até 30 (trinta) usuários da PREFEITURA;

7.4.5.7. Implementação da solução de Proteção DNS recursivo para até 50 (cinquenta) alunos da PREFEITURA.

7.4.5.8. Documentação;

7.4.5.9. Transferência de conhecimento de até 24 (vinte e quatro) horas para os colaboradores da PREFEITURA.

## 7.5. MANUTENÇÃO E SUPORTE TÉCNICO

7.5.1. A solução fornecida deverá possuir garantia de funcionamento, serviços de manutenção e suporte técnico, por um período de 48 (quarenta e oito) meses, a contar da data de emissão do termo de aceite do produto.

7.5.2. O Serviço de manutenção e suporte técnico deverá abranger a manutenção corretiva com cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a substituição de peças, partes, componentes e acessórios.

7.5.3. A modalidade de suporte a ser disponibilizado deverá ser 24x7 (24 horas por dia, 07 dias por semana) de responsabilidade da CONTRATADA.

7.5.4. Caso haja eventual indisponibilidade nas Soluções de Subscrição ou SaaS e esta indisponibilidade superar o prazo de 06 (seis) horas, a CONTRATADA deverá apresentar todas as devidas justificativas do Fabricante à PREFEITURA, além de acompanhar a evolução da restauração completa do serviço, para que não ocorra penalidades.

7.5.5. A CONTRATADA deverá assegurar a assistência técnica necessária e satisfatória das soluções, no que consiste à manutenção, reinstalação e atualização de softwares/firmwares das soluções.

7.5.6. Para prestação do serviço de garantia será exigido que a CONTRATADA habilite o suporte junto ao Fabricante, para todos as soluções relacionadas

7.5.7. A CONTRATADA deverá disponibilizar para a PREFEITURA, durante o período de vigência da garantia, acesso automático às documentações e as versões de manutenção e atualizações de software/firmwares dos PRODUTOS, via portal web internet do fabricante, sob demanda, sem ônus à PREFEITURA.

7.5.8. A CONTRATADA deverá ter acesso direto ao suporte técnico especializado do Fabricante dos PRODUTOS, via telefone e e-mail, para solução dos problemas e encaminhamento dos problemas ao setor competente do Fabricante. Deve também disponibilizar uma senha de acesso para este serviço a equipe da PREFEITURA.

7.5.9. A CONTRATADA acionará através de abertura e acompanhamento de chamados o centro de suporte técnico do Fabricante, bem como acompanhamento da resolução desses chamados e implantação das soluções sugeridas pelo Fabricante.

7.5.10. A assistência técnica da CONTRATADA deverá cobrir atendimento telefônico, sem limitação, durante

a vigência do contrato.

7.5.11. O Fornecimento e instalação de atualizações corretivas e evolutivas de programas (tais como firmware e sistema operacional dos produtos), sempre que solicitadas pela PREFEITURA, necessárias ao bom funcionamento das soluções.

7.5.12. Qualquer atualização nos EQUIPAMENTOS somente será feita mediante conhecimento prévio da PREFEITURA;

7.5.13. A CONTRATADA prestará os serviços de manutenção corretiva e suporte técnico das soluções contratadas, independentemente dos acessórios ou outros equipamentos que estejam a este conectados.

7.5.14. É facultado à PREFEITURA realizar a manutenção de primeiro nível nas soluções, desde que executado por pessoal técnico devidamente treinado para realização dos serviços, não eximindo a CONTRATADA de quaisquer responsabilidades sobre o reparo nas soluções.

7.5.15. A CONTRATADA deverá disponibilizar número de telefone 0800 ou telefone com tarifação local da cidade de São Paulo, e-mail, além de sistema de abertura de chamados web à PREFEITURA.

7.5.16. A CONTRATADA deverá possuir número de telefone e fax com tarifação local da cidade de São Paulo ou serviço de Call Center 0800 (sem custo na ligação para a PREFEITURA) equivalente caso seja tarifação diferencial a localidade de São Paulo.

7.5.17. A CONTRATADA deverá possuir base de suporte ou equivalente num raio de até 100 km da sede da PREFEITURA para conseguir cumprir o atendimento dentro do prazo estabelecido.

## 8. SOLUÇÃO DE MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES

### 8.1. REQUISITOS DO NEGÓCIO

8.1.1. Contratação de empresa para fornecimento de solução de APM (Application Performance Management), incluindo treinamento, serviços de implantação e suporte técnico. A solução de APM deverá atender aos requisitos de Monitoramento de aplicações em tempo real, que inclui Desempenho, Disponibilidade, Usabilidade e Segurança das Aplicações dispostas no ambiente da PREFEITURA.

### 8.2. HARDWARE E SOFTWARE

8.2.1. A Solução deve ser entregue com licenças como subscrição, no modelo de Software como Serviço em nuvem (SaaS).

8.2.2. Todo o licenciamento da solução deve ser entregue via subscrição com validade mínima de 48 (quarenta) meses e suporte com atendimento 24x7 incluso.

8.2.3. O suporte deve ser ter validade mínima de 48 (quarenta e oito) meses.

8.2.4. A plataforma SaaS deve obrigatoriamente estar disponível em nuvem pública (IaaS) suportada pelo próprio fabricante da solução ou nuvem privada do Fabricante.

8.2.5. A plataforma SaaS deve prover resiliência em três zonas distintas em uma mesma região (modelo ativo/ativo)

8.2.6. A plataforma SaaS deve ser certificada pelas seguintes regulamentações: SOC 2 Type II e ISO 27001.

8.2.7. O item que compõe a solução de monitoração de performance deverá atender completamente aos requisitos desta Especificação Técnica sem necessidade de quaisquer outras ferramentas complementares.

8.2.8. A proposta da licitante deverá vir acompanhada de documentação técnica que comprove o

atendimento de todos os requisitos deste TR.

8.2.9. A licença de software deverá ser ofertada na modalidade de subscrição (assinatura), ou seja, o CONTRATANTE terá o direito de utilizar a solução de APM enquanto vigorar o CONTRATO.

8.2.10. As subscrições de software deverão ser ofertadas na modalidade SaaS (Software as Service), ou seja, a CONTRATADA deverá prover a infraestrutura para armazenamento da informação e consoles de consulta em estrutura própria com acesso pela internet.

8.2.11. Todos os componentes de software, licenças e suporte necessários para utilização da solução, considerando requisitos recomendados pelo fabricante para uma adequada monitoração do ambiente, incluindo os bancos de dados para armazenamento das informações, deverão estar incluídos na solução ofertada.

8.2.12. A nuvem pública será responsável pela segurança das informações da PREFEITURA armazenadas nos provedores de nuvem.

8.2.13. A solução deverá ser ofertada em sua última versão estável.

8.2.14. O software de APM não poderá constar, no momento da apresentação da proposta técnica, em listas de fim de suporte pelo fabricante, isto é, deve ser produto de uso corrente, sem previsão de descontinuidade de fornecimento ou suporte.

8.2.15. A empresa contratada deverá disponibilizar o item de Solução de APM em até 15 (quinze) dias úteis após a assinatura do contrato.

8.3. **QUANTIDADE DE SERVIDORES E LICENCIAMENTO DA SOLUÇÃO**

8.3.1. A solução de APM deverá ser implantada em um ambiente de nuvem ou on-premises.

8.3.2. A solução ofertada deverá vir licenciada para 01 (um) host de Aplicações, contendo pelo menos os seguintes serviços abaixo:

8.3.2.1. Monitoramento de Performance de Aplicações

8.3.2.2. Visibibidade em tempo real de saúde e desempenho dos servidores

8.3.2.3. Fornecer visibilidade em tempo real de redes dos servidores

8.3.2.4. Análise de transações

8.3.2.5. Análise de vulnerabilidades e proteção de aplicações em runtime

8.3.2.6. Características dos servidores:

| **Servidores de Aplicações (1 servidor para todas as aplicações):** | |
|---|---|
| SO e versão | SO e versão |
| Framework / WebServer e versão | IIS 10.0.17763.1 |
| Liguagem | .NET (MVC / Webforms) |
| Infra Plataforma | VM em KVM (Nutanix) |

| | |
|---|---|
| Quantidade de vCPU | 12 |
| Quantidade de Memória (em GB) | 64 |

8.3.3. A solução ofertada deverá vir licenciada para 01 (um) host de Banco de Dados, para atender aos seguintes itens:

8.3.3.1. Visibilidade em tempo real de saúde e desempenho dos servidores

8.3.3.2. Fornecer visibilidade em tempo real de redes dos servidores

8.3.3.3. Monitoramento de banco de dados

8.3.3.4. Características dos servidores:

| **Servidor de Banco de Dados** | |
|---|---|
| SO e versão | SO e versão |
| DB Versão | QL Server 2019 Standard |
| Infra Plataforma | VM em KVM (Nutanix) |
| Quantidade de vCPU | 40 |
| Quantidade de Memória (em GB) | 120 |

8.3.4. A solução deve ser capaz de monitorar a experiência do usuário final para sistemas Web partindo-se do navegador sem a necessidade de intervenção do usuário como instalação de agente ou extensão de navegador. Deve monitorar a experiência do usuário de pelo menos 10.000.000 (dez milhões) de page views por ano;

8.4. **CARACTERÍSTICAS ESPECÍFICAS DA PLATAFORMA**

8.4.1. O monitoramento de componentes de infraestrutura (rede, memória, CPU, máquinas virtuais, orquestrador de contêineres e banco de dados) deverá estar contemplado, sem custo, sem que seja necessária a instalação de clientes adicionais para monitoração desses componentes. Além da monitoração de experiência do usuário final.

8.4.2. A solução deverá ser ofertada em sua última versão estável.

8.4.3. A solução deverá monitorar aplicações heterogêneas, hospedadas em ambiente de nuvem ou no Datacenter da Contratante.

8.4.4. A solução deverá permitir flexibilidade no licenciamento de agentes independente de tecnologia e/ou linguagem de aplicações, possibilitando a reutilização de uma licença em diferentes tecnologias e/ou aplicações, respeitado o limite contratado.

8.4.5. A solução deverá permitir identificar claramente os problemas ou incidentes ocorridos, com uso de inteligência artificial, nas aplicações hospedadas no ambiente do Data Center, identificando a causa raiz do problema, indicando em qual camada ocorreu o problema (exemplo: aplicação, serviço, webservice, servidor,

web, rede, usuário) e qual o impacto causado pelo problema, indicando usuários, serviços, SLOs, aplicações afetadas.

8.4.6. A solução deverá, de forma automática com uso de inteligência artificial, identificar os problemas que estão ocorrendo no ambiente, analisando automaticamente todos os incidentes relacionamentos entre todos os componentes, de forma a apontar os problemas agrupados, separando causa e efeito. Deverá fazer isso em tempo real e manter o histórico dos problemas ocorridos.

8.4.7. A solução deverá realizar a correlação automática de eventos e análise aprofundada do desempenho e disponibilidade das aplicações, podendo chegar até o nível de classes e métodos da aplicação.

8.4.8. A solução deverá, automaticamente e de forma gráfica, correlacionar todos os componentes, incluindo, hosts, processos, serviços e aplicações e suas dependências. Deverá permitir filtros em qualquer tipo de componente identificado, de forma que a solução exiba todos os componentes que se relacionam ou estão relacionados com o componente filtrado.

8.4.9. Todos os componentes da solução devem ser implantados em ambiente do SaaS seguro na nuvem da fabricante em território brasileiro.

8.4.10. Não serão aceitas soluções que demandem uso de espelhamento/mirror/span de dados de rede (incluindo de redes virtualizadas).

8.4.11. Não serão aceitas soluções que requeiram acesso privilegiado (root) para execução dos agentes.

8.4.12. A solução deve monitorar as aplicações dinamicamente, utilizando tecnologia de bytecode.

8.4.13. Deve haver criptografia nativa da solução para a comunicação ponto a ponto entre todos os componentes/módulos da solução.

8.4.14. A interface de administração e operação da solução deve ser 100% WEB (sem demandar instalação de clientes em estações).

8.4.15. A solução deverá prover aplicativo Mobile (iOS e Android) para visualização de informações referentes ao desempenho das aplicações e aplicativos Mobile monitorados, saúde das transações de negócio, alertas, eventos e dashboards.

8.4.16. A solução deverá oferecer um editor que permita a criação de dashboards, painéis personalizados permitindo a inclusão de imagens, labels, iFrames, e permitindo também a configuração da navegação em fluxo, Drill Downs customizados entre dashboards e entidades.

8.4.17. Os dashboards deverão permitir a extração de dados da integridade operacional, desempenho do aplicativo, infraestrutura e dados relevantes de negócios.

8.4.18. A solução deverá possibilitar que os Dashboards contenham vários widgets, gráficos comuns de barras e porcentagens, gráficos de séries temporais, histogramas e gráficos variados, permitindo também a inclusão de imagens customizadas e links para a criação de um fluxo de navegação entre dashboards e entidades.

8.4.19. O acesso a dashboards deverá ser limitado a grupos específicos ou compartilhado para permitir acesso sem exigir autenticação. Além disso, os painéis deverão ter a possibilidade de ser executados e entregues como relatórios periódicos.

8.4.20. A solução deverá prover suporte a autenticação em OpenLDAP, Microsoft Active Directory e SAML (ou outro método similar), suportando, minimamente:

8.4.20.1. A autorização deverá ser feita por meio de controles de acesso baseados em função (Roles) que

possuindo permissões refinadas, permitindo a aplicação das permissões no nível da aplicação ou camada individual da aplicação.

8.4.20.2. A solução deverá possuir segregação de acesso por aplicação monitorada e por tipo de permissão (apenas visualização e edição);

8.4.20.3. A solução deverá instrumentar e monitorar aplicações nas plataformas indicadas sem demandar alterações no código fonte das aplicações.

8.4.21. A monitoração da aplicação deve ser iniciada de forma automática, junto com a inicialização do servidor de aplicações.

8.4.22. A solução deverá possuir mecanismos de visualização de dados históricos sem a necessidade de leitura de arquivos externos à solução;

8.4.23. Deve descobrir automaticamente e dinamicamente a topologia da aplicação alvo, contendo a comunicação entre seus componentes, apresentando um mapa completo da aplicação.

8.4.24. Esta descoberta deverá ser realizada de forma automática e constante, atualizando dinamicamente no evento de alterações na aplicação (sem intervenção manual do analista/usuário).

8.4.25. O mapa deverá ser apresentado em tela única, sem demandar múltiplos “drill-downs” para sua visualização.

8.4.26. A solução deverá ter a capacidade de apresentar o mapa da aplicação em diferentes períodos (por exemplo, mapa atual e mapa da semana passada).

8.4.27. Esta descoberta automática deverá suportar, no mínimo, os seguintes protocolos/tecnologias/chamadas:

8.4.27.1. HTTP/HTTPS;

8.4.27.2. Web Services;

8.4.27.3. Banco de Dados;

8.4.27.4. Serviços de Mensageria (exemplo: MQ);

8.4.27.5. Cache;

8.4.27.6. LDAP/Active Directory.

8.4.28. Para todos os elementos descobertos, deverá ser monitorado o volume de chamadas e seu tempo de resposta.

8.4.29. A descoberta deverá permitir o correlacionamento automático das informações de componentes de plataformas distintas (exemplo: correlacionar as informações coletadas de uma aplicação de front-end PHP consumindo um WEB Service JAVA).

8.4.30. A solução deverá realizar a descoberta automática e o monitoramento de chamadas a elementos externos ao ambiente do CONTRATANTE (exemplo: chamadas de Web Service para servidores remotos em que não é possível a instalação de agentes (serviços de terceiros, etc.)).

8.4.31. O mapa deverá apresentar o volume de execuções e tempos médio de resposta entre todos os componentes da aplicação de acordo com o período selecionado pelo usuário/analista.

8.4.32. O mapa deverá apresentar de forma visual eventuais desvios no comportamento da aplicação (por exemplo, problemas de performance na comunicação entre dois componentes).

8.4.33. Deve descobrir automaticamente transações de negócio (ações resultantes da interação com usuários ou sistemas)

8.4.34. Deverá detectar transações de negócio de forma automática, iniciadas com base nos seguintes protocolos/tecnologias:

8.4.34.1. Chamadas Web (HTTP/HTTPS);

8.4.34.2. Web Services;

8.4.34.3. Serviços de Mensageria (exemplo: MQ);

8.4.34.4. EJB – Enterprise JavaBeans;

8.4.34.5. Spring Bean;

8.4.34.6. Struts Action;

8.4.35. A solução deverá também suportar a configuração de início de transação por qualquer classe/método da aplicação.

8.4.36. No caso de aplicações que utilizam protocolos de comunicação ou mensagens customizados (Ex: Socket TCP) a solução deverá prover funcionalidade para que seja feita a configuração da correlação das camadas da aplicação via configuração ou utilização de SDK próprio para personalização.

8.4.37. A solução, após ter realizado a descoberta das aplicações e transações, deverá:

8.4.38. Apresentar um mapa específico da topologia da transação de negócio, com as mesmas funcionalidades do mapa de aplicação;

8.4.39. Deve descobrir o fluxo e arquitetura completo da Transação de Negócio, com suporte para transações síncronas, assíncrona e com múltiplas threads.

8.4.40. Monitorar 100% das execuções da transação de negócio, contendo minimamente as seguintes métricas:

8.4.40.1. Volume de execuções da transação;

8.4.40.2. Tempo de resposta médio;

8.4.40.3. Volume de erros;

8.4.41. A solução deverá classificar e quantificar a execução das transações de acordo com seu tempo de resposta e eventuais erros, de forma a possibilitar ao o usuário/analista a identificação de falhas na linha do tempo (exemplo: 90% das transações normais, 7% com baixa performance, 3% com erro).

8.4.42. Deverá suportar esse tipo de análise em qualquer intervalo de tempo, permitindo, por exemplo, a comparação de performance entre diferentes versões da aplicação (exemplo: últimas quatro horas comparadas com o mesmo intervalo no mês anterior).

8.4.43. A classificação e quantificação deverá ser suportada em nível de aplicação, transação de negócio e servidor de aplicação.

8.4.44. A solução deverá capturar erros e exceções em qualquer ponto da aplicação, permitindo que o usuário/analista identifique o tipo de erro e o ponto da transação de negócio em que ocorreu.

8.4.45. A solução deverá criar métricas de volume de erros por tipo de erro;

8.4.46. A solução deverá monitorar o uso de recursos de infraestrutura do servidor de aplicação (uso de CPU, Memória, I/O de disco e rede), correlacionando os dados coletados com os dados da aplicação no mesmo período.

8.4.47. A solução deverá fornecer a capacidade da importação ou criação de extensões de monitoração customizada, para a monitoração de sistemas internos e proprietário da empresa, através da execução de qualquer script ou programa no servidor, desde que retorne as métricas no formato esperado pelo agente.

8.4.48. A solução deverá prover soluções para a ingestão de métricas externas ou eventos customizados (Ex: Deployment de aplicações)

8.4.49. A solução deverá fornecer ferramentas para entender o uso de memória para otimizá-lo, determinar se o uso de memória está relacionado a um problema e fornecer avisos quando houver indicadores de problemas. Essas ferramentas deverão permitir a detecção de Memory leak permitindo investigar a quantidade de instâncias da classe/objeto que estão relacionados ao Memory Leak.

8.4.50. A solução deve monitorar o comportamento de utilização de memória do servidor de aplicação JAVA, contendo, no mínimo, as seguintes métricas:

8.4.50.1. Percentual de heap utilizada;

8.4.50.2. Execução de garbage colector;

8.4.50.3. Promoção de objetos;

8.4.50.4. O agente deve ser nativamente projetado para minimizar o consumo de recursos, com limite máximo 2% de consumo adicional de CPU.

8.4.51. A solução deverá coletar métricas da JVM via JMX, suportando, minimamente:

8.4.51.1. Métricas de Thread Pool

8.4.51.2. Métricas do pool de conexão JDBC

8.4.51.3. Qualquer outra métrica JMX, numérica, configurável pelo usuário/analista.

8.4.52. A solução deve ser capaz de aprender automaticamente o comportamento das aplicações, e criar o baseline dinâmico de todas as métricas monitoradas pela solução (incluindo estatísticas como uso de CPU, Memória, Heap JVM, métricas de JMX, incluindo qualquer outra definida pelo usuário/analista).

8.4.53. O baseline deverá permitir configuração para detectar desvios de comportamento de qualquer métrica, com base em janelas de tempo distintas (por exemplo: últimas horas, horário de produção, dias do mês, etc.).

8.4.54. A solução deverá apresentar detalhamento de tempos de execução em nível de classe e método para as transações que desviarem do comportamento normal detectado por meio do baseline dinâmico.

8.4.55. Este detalhamento deverá apresentar todos os métodos executados pela aplicação sem a necessidade de configuração manual por parte do usuário/analista.

8.4.56. Não serão aceitas soluções em que deverão ser definidas de forma manual pelo usuário/analista as classes e métodos, exceto para personalização de métricas de negócio.

8.4.57. Este detalhamento deverá conter, tempos de execução com granularidade de classe e método, o mapa completo da transação e correlação real entre múltiplas linguagens, tecnologia, protocolos e camadas da aplicação de uma interação única de um usuário com uma transação de negócio.

8.4.58. Não serão aceitas soluções que apresentam apenas métricas correlacionadas no tempo ou visões detalhadas sem correlação real de uma interação única de um usuário.

8.4.59. Esta correlação deverá ocorrer dinamicamente, constantemente e automaticamente, sem a necessidade de configuração manual ou alteração do código da aplicação, suportando, no mínimo, os seguintes protocolos e tecnologias:

8.4.60. Transações síncronas e assíncronas

8.4.60.1. HTTP e HTTPS

8.4.60.2. WebServices SOAP e REST

8.4.60.3. Serviços de Mensageria

8.4.60.4. Execuções de Queries no Banco de dados

8.4.60.5. Correlação com múltiplas threads

8.4.60.6. Dependência de serviços externos, sem agentes da solução, detectando como backends.

8.4.61. A granularidade de coleta dos métodos em execução deverá ser no máximo de 10ms.

8.4.62. Esta taxa de coleta deve ser mantida mesmo em momentos de alto volume de execução de transações e/ou consumo de CPU, de modo a prover as informações necessárias para o diagnóstico do problema.

8.4.63. Deve ter a capacidade de globalizar a definição de alertas com uma solução de política por aplicação, sem ter a necessidade de configuração de métricas individualmente.

8.4.64. A solução deverá ter a capacidade de retenção mínima de um ano de histórico de métricas.

8.4.65. A granularidade máxima de agregação deverá ser por hora, considerando pelo menos até 365 dias.

8.4.66. Para janelas de tempo mais recentes (até 3 horas atrás), a granularidade máxima deverá ser de até um minuto.

8.4.67. A solução deverá permitir a criação de dashboards/painéis customizados pelo usuário/analista.

8.4.68. A customização de dashboards/painéis deve ser simplificada, sem demandar a alocação de técnicos especializados para desenvolvimento de código ou uso de APIs;

8.4.69. Deve prover diagnósticos em nível de código (visibilidade de classes e métodos) em Transações de Negócio com performance ruim.

8.4.70. Deve identificar Transações de Negócio lentas ou travadas, sem intervenção manual.

8.4.71. Deve identificar queries SQL lentas, sem intervenção manual.

8.4.72. Deve identificar sistemas de backend ou serviços externos lentos, sem intervenção manual

8.4.73. Deve automaticamente descobrir problemas de código, incluindo, no mínimo, deadlocks em aplicações Java.

8.4.74. Deve permitir a criação de métricas customizadas visando prover visibilidade sobre o impacto dos problemas ao negócio da organização.

8.4.75. Estas métricas deverão ser coletadas em tempo de execução com base em parâmetros ou retorno resultantes da execução dos métodos (exemplo: valor do repasse de um determinado recurso financeiro utilizado em um método específico da aplicação)

8.4.76. Essas métricas customizadas deverão suportar baselines e alertas automáticos baseados em desvio de comportamento.

8.4.77. Deve oferecer a facilidade de criar dashboards customizáveis com essas métricas de negócio e correlaciona-las ao comportamento da aplicação.

8.4.78. A solução deverá suportar a criação de métricas de negócios, permitindo alertas sobre alterações nos dados relacionados aos negócios quando existir um desvio de acordo com o Baseline configurado.

8.4.79. Deve fornecer relatórios de desempenho pré-construídos com resumo e tendências das Transações de Negócio

8.4.80. Deve prover automaticamente e dinamicamente baseline de todas as métricas para identificar desvios de comportamento, reduzir alarmes falsos e eliminar definição de parâmetros de limites estáticos.

8.4.81. Deve fazer automaticamente baseline de novos componentes, sem intervenção manual, evitando

grande volume de alertas e falso positivos.

8.4.82. A solução deverá prover baseline de 100% das métricas de forma automática, inclusive as de negócio, permitindo ser configuradas com janelas de tempo de rolagem flexíveis variando de 24 horas a até 1 ano de dados históricos, permitindo também considerar tendências históricas de curto e de longo prazo nos sistemas do cliente.

8.4.83. Deve identificar hotspots da aplicação (rapidamente detectar os métodos da aplicação que demoram mais tempo para serem executados causando problemas de desempenho na Transação de Negócio).

8.4.84. Deve permitir análise de escalabilidade, correlacionando graficamente o tempo de resposta da aplicação com o volume de transações.

8.4.85. Deve identificar as piores chamadas de backend automaticamente (Banco de Dados, Web Services e outros serviços de backend)

8.4.86. A solução deve permitir a criação de alertas, com base em métricas/eventos/situações definidas pelo usuário/analista:

8.4.86.1. Deve possuir a capacidade de criação de alertas com base em métricas estáticas e dinâmicas, resultantes da geração de baseline da solução (exemplo: uso de CPU do servidor de aplicação com mais de três desvios padrão esperados para um determinado período).

8.4.87. Deverá executar ações resultantes da deflagração de um alerta, suportando, no mínimo:

8.4.87.1. Envio de e-mail;

8.4.87.2. Chamada de um Web Service com configuração de parâmetros da chamada diretamente na interface da solução;

8.4.87.3. Execução de um script no servidor da solução, exceto se a solução for em plataforma SaaS;

8.4.87.4. Execução de um script no servidor da aplicação, com o objetivo de remediar incidentes (exemplo: aumento de thread pool, reinicialização da JVM, entre outros).

8.4.88. Deve permitir a criação de alertas para qualquer métrica individual disponível na ferramenta.

8.4.89. Deve permitir a criação de alertas para grupos de métricas configuradas na ferramenta.

8.4.90. Deve permitir a criação de alertas baseados em política por aplicação, sem ter a necessidade de configuração de métricas individualmente (exemplo: um alerta configurado para transações de negócio de uma aplicação será automaticamente aplicado para uma nova transação descoberta pela solução, para a mesma aplicação).

8.4.91. Deve permitir condições, usando lógica E/OU, para disparo de alertas;

8.4.92. Deve permitir desativação de regras de execução de ações temporariamente, para períodos de manutenção.

8.4.93. Deve permitir a classificação de alertas em categorias, de acordo com sua criticidade.

8.4.94. A solução deverá possuir funcionalidade de geração de relatórios.

8.4.95. Deverá permitir o envio de relatórios por e-mail em horários agendados;

8.4.96. Deverá permitir envio de qualquer dashboard/painel criado como um relatório.

8.4.97. Deve possuir facilidade de integração via Rest API

8.4.98. Deve suportar a extração de qualquer métrica da solução para uso na integração com outros sistemas;

8.4.99. As chamadas para API deverão ser autenticadas e criptografadas.

8.4.100. A API deverá suportar consulta de status de regras/alertas configurados na solução.

8.4.101. A solução deve ter a capacidade de monitoração de ambientes monolíticos ou microsserviços (Cloud) com suporte a monitoração de containers docker, em execução em ambientes Kubernetes ou Openshift.

8.4.102. A solução deve ter a capacidade de monitorar o ambiente Kubernetes e Openshift.

8.4.103. A solução deverá prover funcionalidades colaborativas (Ex: possibilidade de compartilhar dashboards ou problemas em uma transação específica com outros usuários através de um botão ou cópia de URL.)

8.5. **CARACTERÍSTICAS GERAIS – BANCO DE DADOS**

8.5.1. A solução deverá fornecer agente para Banco de Dados com suporte específico out-of-the-box para MongoDB, MySQL, SQL Server, Oracle, PostgreSQL, IBM DB2 LUW, Ele deverá fazer Baseline das métricas e as torná-las visíveis em visualizações criadas especificamente, bem como no contexto do aplicativo.

8.5.2. A monitoração do Bando de Dados deverá ocorrer sem a necessidade de instalação de agentes no servidor de Banco de Dados, sendo permitido o uso de agentes nativos ous personalizações (extensions) com acesso remoto ao banco de dados.

8.5.3. Deve gerar baixa sobrecarga, sendo tecnologia segura para monitoramento em produção.

8.5.4. Deve realizar monitoramento de desempenho histórico e tendências.

8.5.5. Deve possuir relatório de principais atividades de banco de dados (por exemplo, Top SQL, Top Users, Top Waiting Status)

8.5.6. Deve possuir relatório de perfil de atividade de banco de dados ao longo do tempo (identificar padrões)

8.5.7. Deve coletar de todos os eventos de wait do banco de dados e correlacionar com SQL/Stored Procedures, sendo permitido o uso de personalizações (extensions).

8.5.8. Deve coletar queries SQL e storage procedures armazenando métricas de performance, incluindo, no mínimo:

8.5.8.1. Volume de execução;

8.5.8.2. Tempo de Execução;

8.5.8.3. Tempo de CPU;

8.5.8.4. Métricas de I/O;

8.5.8.5. Waiting States.

8.5.9. Deve coletar métricas de infraestrutura do servidor/host de banco de dados (CPU, memória, I/O, entre outros), sem a necessidade de instalação de agentes.

8.5.10. Deve fornecer relatórios de comparação de performance e diferentes releases entre períodos distintos, definidos pelo usuário/analista.

8.5.11. Deve realizar a comparação de relatórios das principais queries em execução no banco de dados em períodos distintos, definidos pelo usuário/analista. Deve suportar, no mínimo, os seguintes filtros:

8.5.11.1. Principais queries por volume de execução;

8.5.11.2. Principais queries por tempo de execução

8.5.11.3. Deve realizar a coleta de planos de execução de queries para análise.

8.5.11.4. Deve coletar dados de desempenho de objetos no banco de dados (esquemas, tabelas, índices), sendo permitido o uso de personalizações (extensions).

8.5.12. Deve fornecer uma visão em tempo real do desempenho que mostre a atividade de banco de dados atual

8.5.13. Deve ter a capacidade de enviar alertas proativos, com base na saúde e desempenho de bancos de dados.

8.5.14. Deve fornecer uma visão holística pré-configurada na solução que permita ao usuário/analista entender rapidamente a saúde do banco de dados do ponto de vista de volume de execução, performance e conexões ativas.

8.5.15. A solução deverá prover mecanismo para execução de Querys customizadas através do agente de banco de dados ou qualquer outro tipo de coleta remota com o objetivo de criação de métricas de performance customizadas para o ambiente.

8.5.16. Deve criar baselines de métricas-chave para detecção de desvios de comportamento do bancos de dados.

8.5.17. O sistema de alertas da solução deverá suportar alertas resultantes do monitoramento de bancos de dados.

8.5.18. A solução deve permitir nativamente a criação de dashboards contendo informações tanto do monitoramento de bancos de dados, quanto do monitoramento de aplicações, na mesma visualização.

8.6. **CARACTERÍSTICAS GERAIS – SISTEMAS WEB**

8.6.1. A solução deve ser capaz de monitorar a experiência do usuário final para sistemas Web.

8.6.2. A coleta de informações deverá ocorrer no browser do usuário final, sem a necessidade de instalação de agentes na máquina do usuário, ou de captura de tráfego de rede via espelhamentos/tap/mirror/span.

8.6.3. A solução deverá suportar o monitoramento da experiência do usuário via HTTP e HTTPS.

8.6.4. Não serão aceitas soluções que fazem leitura de tráfego de rede em ponto externo ao servidor de aplicação, com ou sem espelhamento, ou que necessitem descriptografar o tráfego SSL.

8.6.5. A solução deverá monitorar em ambientes Linux com Java a saúde do tráfego de rede entre os componentes da aplicação, fornecendo métricas como:

8.6.5.1. Tempo de Latência

8.6.5.2. Throughput

8.6.5.3. TCP Loss

8.6.5.4. Errors

8.6.5.5. Mapeamento das conexões (Origem, Destino, Porta).

8.6.6. A solução deverá permitir as capturas de pacotes de rede nos nós com o agente instalado (no mínimo para JAVA), sendo permitido o uso de personalizações (extensiond) e, disponibilizar essas capturas preferencialmente por meio da interface WEB para fazer download e encaminhar para os recursos apropriados ou qualquer outro meio que possibilite o download.

8.6.7. A solução deverá monitorar a experiência do usuário em página Web, iFrames e chamadas AJAX.

8.6.8. A solução deverá identificar automaticamente chamadas de tecnologias de SPA (Single-Page App) como React e Angular.

8.6.9. A solução deve identificar/apontar erros de JavaScript que possam interromper a funcionalidade da página e levar a uma má experiência do usuário final.

8.6.10. A solução deverá categorizar a experiência do usuário com base no seu endereço de origem, realizando geolocalização até nível de país e estado.

8.6.11. Deve permitir a configuração de localizações geográficas customizadas, com base em endereços IP privados (RFC 1918).

8.6.12. Deve ser possível, por exemplo, determinar se um determinado grupo de usuários está sofrendo impacto regional devido à degradação de desempenho de sua rede local.

8.6.13. A solução deverá plotar as informações de experiência de usuário coletadas em um mapa global com capacidade de drill-down.

8.6.14. A solução deverá ser capaz de fornecer estatísticas de experiência de usuário categorizadas por, no mínimo, os seguintes indicadores:

8.6.14.1. Tempo total da experiência;

8.6.14.2. Tempo de conexão em rede;

8.6.14.3. Tempo de servidor (execução transacional da aplicação);

8.6.14.4. Tempo de download do HTML e outros recursos da página;

8.6.14.5. Tempo de renderização do browser (DOM Build);

8.6.14.6. Tempo de pós-load.

8.6.15. A solução deverá coletar detalhamento da execução de amostragem de transações para análise específica, contendo:

8.6.15.1. Estatística individualizada da execução da página, com base nos indicadores citados no item anterior.

8.6.15.2. Geolocalização do usuário com detalhamento de país, estado e cidade;

8.6.15.3. Endereço IP de origem do usuário;

8.6.15.4. Informações de sistema operacional, tipo de browser e versões;

8.6.15.5. Detalhamento de performance de outros recursos presentes na página, de forma gráfica na linha do tempo, contemplando, no mínimo: imagens, scripts, CSS e fontes.

8.6.16. A solução deverá monitorar a sessão do usuário em tempo real com o detalhamento das chamadas feitas na aplicação via AJAX, páginas acessadas, eventos do browser do usuário e marcos da experiência do usuário como primeiro byte transmitido e DOM Ready;

8.6.17. Receber informações em tempo real de forma incremental é fundamental para agir rapidamente. Não serão aceitas soluções que não enviam a interação do usuário em tempo real, dentro de uma sessão, e aguardam um tempo de inatividade do usuário para enviar a experiência da sessão completa no final.

8.6.18. A solução deverá ser capaz de correlacionar as informações coletadas da experiência dos usuários com as informações coletadas dos servidores de aplicação e banco de dados.

8.6.19. Esta correlação deverá suportar uma visão fim-a-fim de uma execução única de um usuário (exemplo: possibilidade de realizar um drill-down de uma má experiência do usuário final, até identificar a query no banco de dados que causou o problema).

8.6.20. A solução deverá prover métricas de performance categorizadas, no mínimo, por:

8.6.20.1. Sistema Operacional;

8.6.20.2. Browser;

8.6.21. A solução deverá ser capaz de apresentar gráfico de distribuição de performance dos usuários finais.

8.6.22. O gráfico deverá apresentar, no mínimo, o percentil 99% e 95%.

8.6.23. O gráfico deverá apresentar visualização geral ou por página da aplicação.

8.6.24. A solução deverá prover API em JavaScript para coleta de informações customizadas (exemplo: nome

do usuário, código do cadastro, etc).

8.7. **CARACTERÍSTICAS GERAIS – APPS MOBILE**

8.7.1. A solução deverá suportar a monitoração de aplicativos (Apps) mobile nas plataformas Android e iOS ou Xamarin.

8.7.2. A solução deverá prover informações de experiência dos usuários dos aplicativos, provendo visões do funcionamento do aplicativo em si e da comunicação de rede com aplicações back-end/server side.

8.7.3. A solução deverá correlacionar as chamadas do aplicativo a serviços server side/backend permitindo fazer drill down e análise a nível de código nesses serviços.

8.7.4. A solução deverá possuir a capacidade de rastrear uma requisição desde a ação inicial do usuário, identificando transações de negócio, por todas as camadas da aplicação.

8.7.5. A solução deverá identificar comportamentos de travamentos e crashes no aplicativo e enviar os detalhes para análise posterior, tais como:

8.7.6. Quantidade de usuários afetados por determinado tipo de Crash ou Travamento;

8.7.7. Ações realizadas pelo usuário antes de um Crash

8.7.8. Utilização de memória, operadora, versão do S.O., modelo do telefone e tipo de conexão do aparelho que causou um crash.

8.7.9. Dados customizados de negócio como código do cliente, CPF, etc.

8.7.10. Stack trace completa dos crashes e travamentos

8.7.11. A solução deverá obter dados de utilização e tecnologia utilizadas pelos usuários do App tais como:

8.7.11.1. Aberturas do App por minuto

8.7.11.2. Distribuição de versão do App

8.7.11.3. Crashs e travamentos por versão do App e Modelo de telefone

8.7.11.4. Aberturas de App por país

8.7.11.5. Chamadas a serviços de backend por país

8.7.11.6. Tempo de rede por país

8.7.11.7. Versão dos aplicativos

8.7.12. Operadoras, Modelo do telefone, S.O. e tipos de conexão dos usuários do App;

8.7.13. A solução deve permitir o envio de dados de negócio do aplicativo para a posterior análise, consolidação e visualização analítica.

8.7.14. A solução deve capturar 100% das sessões de utilização do aplicativo e todas as ações realizadas pelo usuário, identificando automaticamente informações como:

8.7.15. Modelo do dispositivo, versão do S.O., geolocalização, tipo de conexão, operadora, versão do aplicativo, endereço, informações de performance das ações, crashes, experiência do usuário final.

8.7.16. A solução deverá permitir a captura automática de ScreenShots do aplicativo durante a utilização do usuário para entendimento do comportamento do usuário final, permitindo ao administrador desabilitar remotamente a captura dos ScreenShots.

8.7.17. A solução deve fornecer insights em tempo real sobre o desempenho da aplicação, visualizando as principais jornadas do usuário e a correlação entre desempenho e tráfego.

8.8. **CARACTERÍSTICAS GERAIS – SISTEMAS NÃO WEB E EMBARCADOS**

8.8.1. A solução deverá suportar a instrumentação de componentes não-web como escritos em C++ ou dispositivos conectados (IoT), Kiosks ou embarcados a partir de SDKs C++, JAVA ou diretamente via Rest API, correlacionando com as chamadas para camadas de backend.

8.8.2. A solução deverá possibilitar aplicações ou componentes não-web e embarcados a enviar dados de negócio ou customizados para serem tratados e exibidos em visões analíticas.

8.8.3. A solução deve possuir interface para visualização de devices conectados (IoT) e suas informações como versão do firmware, quantidades de dispositivos conectados e etc.

8.9. **CARACTERÍSTICAS GERAIS – INFORMAÇÕES DO NEGÓCIO**

8.9.1. A solução deverá ser capaz de extrair métricas referentes ao comportamento do negócio em tempo real (ex: total em reais investido por transação, total em reais investido pelos principais clientes, total em reais distribuído por região e totais em reais perdidos devido a transações problemáticas).

8.9.2. A solução deverá oferecer a capacidade de capturar dados de método com instrumentação a nível de bytecode, headers e parâmetros HTTP sem exigir alterações de código, associando esses dados à transação de negócios e permitindo que esses dados sirvam como fonte de informações para métricas, consultas e sejam exibidos em Dashboards, permitindo também a visualização por exemplo do impacto da receita proveniente de erros nas transações, alterações de código e de mudanças nos processos de negócios em tempo real.

8.9.3. Todas as configurações necessárias deverão ser feitas via interface web, sem a necessidade de instalação de cliente local, arquivos de configuração ou alteração do código fonte.

8.9.4. A solução deverá ser flexível na gestão de métricas permitindo o cálculo de expressões matemáticas das métricas disponíveis tanto para exibição em dashboards quanto como condição para geração de alertas.

8.9.5. A solução deverá permitir a criação de Baselines também das métricas de negócio.

8.9.6. A solução deverá permitir a criação de Baselines com diferentes períodos, sendo permitido personalizações e automação na solução.

8.9.7. A solução deverá ser capaz de identificar desvios de comportamento do negócio, permitindo a tomada de decisões em tempo real pelas áreas competentes.

8.9.8. Todos os componentes responsáveis pela monitoração do negócio devem fazer parte da plataforma na mesma interface (não serão aceitas ferramentas terceirizadas para realizar a coleta, exibição ou análise dos dados.

8.9.9. Os dados de negócio devem ficar disponíveis para a ferramenta de dashboard da própria solução. Não serão aceitas soluções terceirizadas para a criação de dashboards.

8.9.10. A solução deverá apresentar uma interface de pesquisa com opção de criação de queries (ao estilo SQL) ou outros tipos de expressões para consultas avançadas sobre qualquer dado coletado, possibilitando aplicar determinada consulta em gráficos e dashboards, além de permitir utilizar seu resultado para a criação de uma nova métrica.

8.9.11. A solução deverá ser capaz de gerar automaticamente métricas de percentual de conversão para determinada transação de negócio, bem como visualização do funil com todas as etapas e transações de negócio com métricas de abandonos com possibilidade de drill down para as transações de abandono.

8.9.12. A solução deverá ser capaz de consolidar em um único local a experiência e tempo de jornada do usuário dentro de um fluxo de negócio corporativo (ex: monitorar de forma integrada todas as etapas que compõem uma ação de ativação de uma linha telefônica, como:

8.9.12.1. Solicitação de Portabilidade;

8.9.12.2. Validação Dados cadastrais;

8.9.12.3. Aprovação manual Backoffice;

8.9.12.4. Provisionamento da linha, calculando e fornecendo métricas do tempo individual de cada passo, para cada usuário e tempo total de conclusão do fluxo considerando todas as etapas. Para casos onde as transações demoram dias para serem concluídas a coleta será através de informações fornecidas por aplicações diferentes, sendo permitido o uso de personalizações (extensions) para a catpura dos dados em fontes externas, tais como arquivos de logs, repositório de métricas, etc.

8.9.13. A solução deve prover mecanismo para gestão de Metas de experiência do usuário customizadas, podendo ser metas incluindo métricas técnicas ou de negócio, permitindo a aplicação de filtros e comparação com o período anterior (em % de desvio), permitindo a gestão eficaz de indicadores como: O tempo de envio de ordem está em quantos % da meta projetada? Quantos % acima ou abaixo do período anterior?

8.9.14. O monitoramento dos fluxos de negócios deve ser capaz de se integrar com ferramentas terceiras através de coleta de logs e disponibilizar integrações através de API Rest.

8.10. **SEGURANÇA E ANÁLISE DE VULNERABILIDADE DAS APLICAÇÕES**

8.10.1. A solução deve analisar o código em tempo de execução, indicando possíveis vulnerabilidades, reportando o código CVE (Common Vulnerabilities and Exposures) e o código CWE (Common Weakness Enumeration) quando disponível.

8.10.2. A solução deve verificar e informar se houveram ataques nas vulnerabilidades encontradas.

8.10.3. Visando o baixo impacto no ambiente, o mesmo agente deve fazer a monitoração de performance e de segurança da aplicação em execução.

8.10.4. Ao analisar a segurança do código em tempo de execução, a solução deve indicar a aplicação e qual componente da sua arquitetura está sendo impactado, facilitando assim a análise de impacto e priorização da solução.

8.10.5. A solução deve permitir a configuração para o bloqueio automático dos ataques nas vulnerabilidades.

8.10.6. Para as vulnerabilidades descobertas é desejável que seja recomendada uma solução, por exemplo sugerir um upgrade de biblioteca.

8.10.7. A solução deve correlacionar as vulnerabilidades com a topologia da aplicação monitorada, entregando a visibilidade unificada da performance e segurança da aplicação em uma única solução do mesmo fabricante.

8.10.8. Deve ser possível configurar políticas para determinar qual a ação será realizada nas vulnerabilidades e ataques identificados, onde estas políticas podem ser ignorar, detectar ou bloquear a vulnerabilidade ou ataque.

8.10.9. A solução deve possuir capacidade de enviar os eventos de segurança das vulnerabilidades e ataques identificados para a solução Splunk.

8.10.10. A solução deve fornecer um painel em tempo real com a visibilidade da integridade da segurança das

aplicações.

8.10.11. A solução deve fornecer uma lista das bibliotecas que estão em uso pelas aplicações e destacar as vulnerabilidades e riscos introduzidos pelo uso dessas bibliotecas.

8.10.12. Deve possuir a capacidade de configuração de perfil de acesso nas funcionalidades de segurança.

8.10.13. As vulnerabilidades encontradas devem conter categorização atrelada a sua severidade, classificada pelo padrão de especificação CVSS v3.0.

8.10.14. As vulnerabilidades encontradas devem conter descrições detalhadas e referencias atualizadas.

8.10.15. Em caso de ataque, a solução deve possibilitar a coleta e análise de informações detalhadas, permitindo a rápida identificação da aplicação afetada, do status atual do ataque, da origem do ataque, das vulnerabilidades usadas no ataque (caso existam), do componente da aplicação afetado, da severidade do evento, do período ocorrido e a política de segurança ou ação realizada como resposta.

8.10.16. Deve ser capaz de observar eventos em tempo real que não são classificados como ataques, mas que podem impactar a segurança, como a execução de instruções SQL não parametrizadas, exceções de I/O ou problemas de permissão de acesso a arquivos.

8.11. **CARACTERÍSTICAS GERAIS – ARQUIVOS DE LOG**

8.11.1. Deve ser capaz de coletar e armazenar o conteúdo de arquivos de log dos servidores monitorados.

8.11.2. Deve ser capaz de filtrar o conjunto de resultados da leitura do arquivo de log usando o construtor de consulta da solução, baseado em texto.

8.11.3. Deve ser capaz de extrair qualquer campo do arquivo de log para processamento.

8.11.4. Deve ser capaz de realizar mascaramento de campo ou a remoção de dados confidenciais e gerenciar os fusos horários dos registros capturados.

8.11.5. Deve ser capaz de receber mensagens syslog de uma origem remota (conexão TCP) ou do mesmo host onde o agente está instalado.

8.11.6. Deve ser capaz de utilizar expressões regulares para a configuração da leitura do conteúdo do arquivo de log.

8.11.7. A PREFEITURA requer que a Plataforma para o ambiente de Produção/Teste:

8.11.7.1. Tenha capacidade para receber ingest de logs de no mínimo 40 Gb/dia de logs;

8.11.7.2. Tenha retenção mínima de logs por no mínimo 30 (trinta) dias para análise de logs (Log Analytics).

8.12. **MONITORAÇÃO DE SERVIÇOS E APIS EXTERNAS**

8.12.1. A solução deve suportar a visibilidade sobre o desempenho de serviços digitais, portais institucionais externos e internos alojadas na nuvem privada nuvens públicas.

8.12.2. A solução deve ter a capacidade de fornecer informações para avaliar o desempenho da rede entre dois sites físicos, de forma a ter métricas de throughput bidirecionais e métricas de conectividade entre os diferentes sites.

8.12.3. A solução deve suportar pontos de presença (agentes) em vários locais de mundo, incluindo o Brasil.

8.12.4. Para ter suporte para executar os testes sintéticos a solução deve possuir agentes que possam ser instalados no ambiente de datacenter da contratante e em máquinas de usuários.

8.12.5. A solução deve possuir agentes que podem ser instalados em ambientes internos (hosts, desktops).

Esses agentes devem a ter a capacidade de, a partir da definição de uma URL, monitorar a experiência do usuário fim a fim.

8.12.6. A solução deve permitir a execução de testes sintéticos agendados.

8.12.7. A comunicação entre os agentes e o ambiente SaaS do fabricante deve ser HTTPS.

8.12.8. Como resultado dos testes executados, a solução deve suportar mostrar no mínimo as seguintes informações:

8.12.8.1. Métricas de latência, jitter e perda de pacotes no processo de conexão entre o agente de origem e o servidor de destino.

8.12.8.2. Um mapa gráfico da rota percorrida (nós) entre o site de origem e o servidor de destino, incluindo os diferentes saltos de conectividade, que podem ou não ser através de um link MPLS, conexão via VPN e / ou pela Internet.

8.12.8.3. Validação da disponibilidade do servidor destino.

8.12.8.4. Degradação da rede ao longo do percurso seguido. Esta degradação pode ser determinada de acordo com parâmetros definidos como níveis máximos aceitáveis.

8.12.8.5. Visibilidade do tráfego entre ISPs (Provedores de Serviços de Internet).

8.12.8.6. A solução deve permitir que um mesmo teste seja executado por agentes na nuvem ou on premises. Essa configuração deve ser feita na interface da solução

8.12.9. A solução deve permitir a identificação de falhas de conexão com provedores externos, e preferencialmente identificar se existem problemas de comunicação entre os saltos.

8.12.10. Para cada teste de executado a solução deve guardar as métricas e exibi-las na linha do tempo para uma fácil investigação e detecção de causa raiz.

8.12.11. A solução deve permitir a mensuração de métricas de DNS.

8.12.12. A solução deve permitir que dados necessários a identificação e correção de problemas sejam compartilhados de forma simples.

8.12.13. A solução deve possuir a capacidade de descobrir pro ativamente falhas em provedores de serviço externos na internet.

8.12.14. A solução deve possuir APIs que permitam a extração da dados e interação com outras ferramentas.

8.12.15. A solução deve permitir a simulação de um usuário real interagindo com uma aplicação web através de um browser. Por exemplo, acessar a página de login, após o login executar uma consulta de saldo e depois fazer logoff.

8.12.16. Ao monitorar serviços HTTP, a solução deve prover no mínimo as métricas abaixo: Disponibilidade, Response Code, Response Time, DNS Time, Connect Time, SSL Negotiation Time, Wait Time, Receive Time, Total Time.

8.12.17. Ao monitorar o carregamento de uma página (Page Load) a solução deve trazer na interface gráfica o detalhamento de todos os componentes que foram carregados.

8.12.18. A solução deve permitir a criação de um único dashboards contendo informações sobre a infraestrutura, as aplicações e os testes sintéticos.

8.13. **SERVIÇO INSTALAÇÃO DA SOLUÇÃO PERFORMANCE DE APLICAÇÃO**

8.13.1. A CONTRATADA deverá atender aos seguintes requisitos para instalação e entrega do serviço:

8.13.1.1. Ter pelo menos um profissional certificado na solução, através de comprovação expedida pelo Fabricante da solução;

8.13.1.2. O serviço de instalação e configuração compreende desde a configuração lógica, testes, até que a solução esteja ativa e em pleno funcionamento. Caberá a CONTRATADA realizar a instalação da solução nas dependências da PREFEITURA de acordo com a seguinte metodologia de trabalho:

8.13.1.3. Reunião preliminar com a equipe técnica da PREFEITURA para definir o escopo de serviços da instalação;

8.13.1.4. Elaboração e entrega de pré-projeto de instalação contendo as configurações principais a serem aplicadas e o cronograma de trabalho para aprovação da PREFEITURA;

8.13.2. A PREFEITURA entende que para a execução dos serviços de instalação e configuração definidos para implantação do projeto a CONTRATADA deve contemplar no mínimo de 350 (trezentos e cinquenta) horas comerciais, podendo ser distribuídas em horas locais na PREFEITURA ou remoto, e 32 (trinta e duas) horas fora do horário comercial;

8.13.3. Acompanhamento da instalação da solução (dentro das quarenta horas prevista).

8.13.4. O serviço deve incluir as seguintes configurações:

8.13.4.1. Levantamento do Ambiente, Requisitos e Conversas com os Proprietários de Aplicativos;

8.13.4.2. Planejamento e Preparação Inicial da Documentação do Projeto;

8.13.4.3. Provisionamento da Solução SaaS no Fabricante;

8.13.4.4. Instalação de Agentes e Configuração no Servidor de Aplicações, e Servidor de Banco de Dados;

8.13.4.5. Janela de manutenção para a implementação da solução, com instalação de Agentes e configuração de Servidores;

8.13.4.6. Configurações e ajustes finos;

8.13.4.7. Configuração de Alertas Personalizados e Dashboard;

8.13.4.8. Mapeamento de Métricas, criação e configurações para Analíticos de Negócios;

8.13.4.9. Documentação;

8.13.4.10. Transferência de Conhecimento (handson) no Ambiente da PREFEITURA.

## 8.14. MANUTENÇÃO E SUPORTE TÉCNICO

8.14.1. A solução fornecida deverá possuir garantia de funcionamento, serviços de manutenção e suporte técnico, por um período de 48 (quarenta e oito) meses, a contar da data de emissão do termo de aceite do produto.

8.14.2. O Serviço de manutenção e suporte técnico deverá abranger a manutenção corretiva com cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a substituição de peças, partes, componentes e acessórios.

8.14.3. A modalidade de suporte, de responsabilidade da CONTRATADA, disponibilizar atendimento 24x7 (24 horas por dia, 07 dias por semana) com início do tratamento do chamado para o próximo dia útil;

8.14.4. Em eventual indisponibilidade da Solução de Subscrição ou SaaS, a CONTRATADA deverá apresentar as justificativas do Fabricante à PREFEITURA, além de acompanhar a evolução da restauração completa do serviço, para que não ocorra penalidades.

8.14.5. A CONTRATADA deverá assegurar a assistência técnica necessária e satisfatória das soluções, no

que consiste à manutenção, reinstalação e atualização de softwares/firmwares das soluções.

8.14.6. Para prestação do serviço de garantia será exigido que a CONTRATADA habilite o suporte junto ao Fabricante, para todos as soluções relacionadas

8.14.7. A CONTRATADA deverá disponibilizar para a PREFEITURA, durante o período de vigência da garantia, acesso automático às documentações e as versões de manutenção e atualizações de software/firmwares dos PRODUTOS, via portal web internet do fabricante, sob demanda, sem ônus à PREFEITURA.

8.14.8. A CONTRATADA deverá ter acesso direto ao suporte técnico especializado do Fabricante dos PRODUTOS, via telefone e e-mail, para solução dos problemas e encaminhamento dos problemas ao setor competente do Fabricante. Deve também disponibilizar uma senha de acesso para este serviço a equipe da PREFEITURA.

8.14.9. A CONTRATADA acionará através de abertura e acompanhamento de chamados o centro de suporte técnico do Fabricante, bem como acompanhamento da resolução desses chamados e implantação das soluções sugeridas pelo Fabricante.

8.14.10. A assistência técnica da CONTRATADA deverá cobrir atendimento telefônico, sem limitação, durante a vigência do contrato.

8.14.11. O Fornecimento e instalação de atualizações corretivas e evolutivas de programas (tais como firmware e sistema operacional dos produtos), sempre que solicitadas pela PREFEITURA, necessárias ao bom funcionamento das soluções.

8.14.12. Qualquer atualização nos EQUIPAMENTOS somente será feita mediante conhecimento prévio da PREFEITURA;

8.14.13. A CONTRATADA prestará os serviços de manutenção corretiva e suporte técnico das soluções contratadas, independentemente dos acessórios ou outros equipamentos que estejam a este conectados.

8.14.14. É facultado à PREFEITURA realizar a manutenção de primeiro nível nas soluções, desde que executado por pessoal técnico devidamente treinado para realização dos serviços, não eximindo a CONTRATADA de quaisquer responsabilidades sobre o reparo nas soluções.

8.14.15. A CONTRATADA deverá disponibilizar número de telefone 0800 ou número de telefone com tarifação local da cidade de São Paulo, e-mail, além de sistema de abertura de chamados web à PREFEITURA.

8.14.16. A CONTRATADA deverá possuir número de telefone e fax com tarifação local da cidade de São Paulo ou serviço de Call Center 0800 (sem custo na ligação para a PREFEITURA) equivalente caso seja tarifação diferencial a localidade de São Paulo.

8.14.17. A CONTRATADA deverá possuir base de suporte ou equivalente num raio de até 100 km da sede da PREFEITURA para conseguir cumprir o atendimento dentro do prazo estabelecido.

8.15. **BANCO DE HORAS DE CONSULTORIA TÉCNICA ESPECIALIZADA PARA A SOLUÇÃO DE PERFORMANCE DE APLICAÇÕES**

8.15.1. A CONTRATADA deverá disponibilizar para a PREFEITURA, 400 (quatrocentas) horas de SERVIÇOS DE CONSULTORIA TÉCNICA ESPECIALIZADA, **sob demanda** e durante a vigência do contrato, devendo disponibilizar Consultor Técnico Especializado;

8.15.2. Entende-se por SERVIÇOS DE CONSULTORIA TÉCNICA ESPECIALIZADA, as atividades de apoio

técnico especializado para ajustes, análises, consultoria, customizações e tunning, instalação e configuração de novas funcionalidades, assesment do ambiente, sempre em conjunto com a Equipe Técnica da PREFEITURA;

8.15.3. Os SERVIÇOS DE CONSULTORIA TÉCNICA ESPECIALIZADA deverão ser executados pela CONTRATADA durante o horário comercial compreendidos entre 8:00 às 17:00hs, de segunda à sexta-feira, devendo eventualmente atender a PREFEITURA em finais de semana e feriados, para atendimento ou acompanhamento de implementações que necessitem serem executados nestes horários, cabendo à PREFEITURA informar tais atendimentos à CONTRATADA antecipadamente e de comum acordo entre as partes;

8.15.4. Para contabilização das horas, será considerado somente o tempo em que no qual o profissional esteve presente, realizando as atividades dentro das instalações da PREFEITURA. Para este controle, o profissional deverá prestar contas diariamente, devendo fornecer o Relatório de Atividades devidamente assinado pelo mesmo e de um profissional da PREFEITURA com o horário de início e término das atividades.

8.15.5. Somente serão aceitas faturas referentes aos Serviços de Consultoria Técnica Especializada prestados, mediante solicitação da PREFEITURA.

## 9. SOLUÇÃO DE MONITORAMENTO DE EXPERIÊNCIA DIGITAL

### 9.1. ESPECIFICAÇÕES TÉCNICAS

**9.1.1. Requisitos Gerais:**

9.1.1.1. A Solução deve possuir vários componentes distintos para atingir os objetivos esperados por este Termo de Referência. Os componentes devem trabalhar em conjunto para fornecer a solução geral;

9.1.1.2. Os seguintes componentes e recursos mínimos devem estar disponíveis na solução ofertada:

9.1.1.3. Agentes para execução de testes;

9.1.1.4. GUI baseada na Web;

9.1.1.5. Dashboard e Relatórios;

9.1.1.6. Alertas para os testes executados a partir dos agentes;

9.1.1.7. Integrações com sistemas e aplicações de terceiros, incluindo uma API REST.

9.1.1.8. Os agentes devem fornecer a compreensão da topologia, dependências e comportamentos da rede, no contexto dos testes executados;

9.1.1.9. A solução deve identificar de forma rápida e precisa a causa raiz dos problemas, no mínimo, para falhas de dispositivos, congestionamentos, ataques DDoS, sequestros de BGP e DNS, vazamentos de rotas, falhas de DNS e interrupções de provedores de serviços;

9.1.1.10. A solução deve compartilhar evidências com fornecedores e parceiros para resolver problemas mais rapidamente. O processo deve permitir o compartilhamento com domínios externos, entidades e clientes, mesmo aqueles que não possuam login/credenciais para acessar a solução;

9.1.1.11. A solução ofertada deverá ser nativamente baseada em SaaS (Software as a Service);

9.1.1.12. A PREFEITURA poderá implantar agentes em sua infraestrutura, mas eles devem incluir apenas um subconjunto da solução geral, sendo que, do ponto de vista da PREFEITURA, a orquestração de testes, o processamento de resultados, relatórios, alertas e integrações, devem ser executados a partir da “nuvem”

(SaaS);

9.1.1.13. A solução ofertada deve ser capaz de identificar a rota de conexão de onde o serviço se origina, para onde é consumido (onde a solicitação é feita), mostrando todos os seus saltos, incluindo sua passagem pela Internet, qualquer perda de pacote que possa ter existido, latência e jitter em cada salto, a fim de identificar se a degradação no serviço tem origem em um ou mais pontos da rota;

9.1.1.14. O recurso de visualização de caminho deve estar disponível como parte da solução;

9.1.1.15. Para cada teste executado deve ser possível visualizar, em uma linha do tempo, os nós reais e links usados no momento do teste, incluindo indicações de problemas, como perda de pacotes e links com latências altas e inesperadas;

9.1.1.16. O recurso de visualização de caminho deve trazer visibilidade de redes e serviços internos e externos;

9.1.1.17. A solução deve ser capaz de gerar testes programados para serviços externos, do tipo SaaS (Software as a Service), utilizados pela PREFEITURA;

9.1.1.18. Os testes especificados para a solução poderão ser executados a partir de sites externos ou internos definidos pela PREFEITURA;

9.1.1.19. No caso de testes executados a partir de sites externos, considera-se que os testes serão realizados através da Internet, enquanto os testes a partir de sites internos poderão ser executados para serviços através da Internet, ou através da rede interna, incluindo meios de conectividade disponibilizados pela PREFEITURA, tais como: Internet e Links do tipo MPLS;

9.1.1.20. No caso de testes a serem executados a partir de sites internos, o recurso a partir do qual são realizados os testes solicitados devem poder ser um servidor virtual, um dispositivo virtual, um servidor físico ou um computador físico.

9.1.1.21. A solução deve coletar, integrar e analisar dados em todos os segmentos de rede e saltos de rede;

9.1.1.22. A solução deve correlacionar, em uma linha de tempo, o desempenho do aplicativo com problemas de infraestrutura. Toda a correlação deve estar disponível em uma GUI como parte da solução;

9.1.1.23. A solução deve ter recursos de Conscientização de Problemas, devendo coletar e apresentar uma visão de ponta a ponta do usuário para o aplicativo, permitindo que os usuários monitorem o caminho da rede em cada “hop” (hop-by-hop), em todas as redes – públicas, privadas e provedoras de serviços – como se todas essas redes fossem corporativas;

9.1.1.24. A solução deve identificar quando uma interrupção do provedor de serviços está afetando os usuários de filiais e, quando um provedor de SaaS tem um problema de roteamento em sua própria rede;

9.1.1.25. A solução deve correlacionar problemas de desempenho e disponibilidade na camada de aplicação, com eventos que ocorrem na camada de rede – para todas as redes, internas e externas.

9.1.1.26. A Solução deve ter recursos de Identificação de Problemas, devendo ter a capacidade de identificar a causa raiz de interrupções de serviços rapidamente e a partir de um único dashboard, minimizando o tempo de solução de problemas e reduzindo a necessidade de contatar vários terceiros para sua própria análise de seus respectivos componentes;

9.1.1.27. Deve permitir que as operações diagnostiquem rapidamente problemas em vários segmentos de rede, serviços e aplicativos, com visualizações que reúnam várias camadas de dados de rede, de várias geografias, em um reduzido número de exibições concisas.

9.1.1.28. A Solução deve ter recursos de Resolução de Problemas, tomando ações após a visualização do

sistema de ponta a ponta, em todos os provedores de rede, mesmo estando a causa raiz em um componente externo, gerenciado por outra empresa, que não a PREFEITURA;

9.1.1.29. A solução deve ser capaz de compartilhar dados e análises abrangentes com as partes envolvidas, para que estas tomem as medidas necessárias para a resolução do problema.

9.1.1.30. A solução deve permitir que a PREFEITURA visualize todas as camadas que compõem sua prestação de serviços em uma única exibição, desde transações sintéticas e disponibilidade de serviços, até caminhos de rede e feeds globais de roteamento da Internet.

9.1.2. **Requisitos de Arquitetura:**

9.1.2.1. A solução deverá utilizar testes sintéticos, gerando um tráfego IP que se assemelha ao tráfego gerado pelo usuário;

9.1.2.2. A execução dos testes deve ser efetuada por um “agente”;

9.1.2.3. A solução deve possuir, no mínimo, os seguintes tipos de agentes para fornecer opções flexíveis de implantação à PREFEITURA:

9.1.2.3.1. "Agentes Internos" – São agentes que deverão ser implantados e gerenciados pela PREFEITURA em suas próprias redes e datacenters, redes de terceiros ou em Nuvens Públicas;

9.1.2.3.2. "Agentes Públicos" – São agentes gerenciados pelo próprio fabricante da solução ofertada, mas que poderão ser utilizados para testes externos pela PREFEITURA. Esses agentes devem estar disponíveis em outros provedores de serviços, operadoras de banda larga e móveis e, no mínimo, nos seguintes provedores de Nuvem Pública Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) e Alibaba Cloud;

9.1.2.3.3. "Agentes de Usuário Final" – São agentes que deverão ser implantados e gerenciados pela PREFEITURA nas estações de trabalho do usuário, para monitorar a Experiência do Usuário Final.

9.1.2.4. Os "Agentes Públicos" deverão ter abrangência global e, estar localizados em, no mínimo, 200 (duzentas) cidades em, no mínimo, 60 (sessenta) países, incluindo o Brasil. A empresa LICITANTE deverá apresentar a lista completa de todos os "Agentes Públicos" disponíveis para a solução ofertada no momento da resposta do edital;

9.1.2.4.1. A PREFEITURA deverá ter acesso a todos os “Agentes Públicos” disponibilizados pelo fabricante da solução ofertada.

9.1.2.5. A solução ofertada deverá suportar, no mínimo, os seguintes cenários de monitoramento de Clouds Públicas, utilizando os “Agentes Públicos”:

9.1.2.5.1. Os “Agentes Públicos” devem possibilitar à solução ofertada o monitoramento Intra e Inter Clouds Públicas;

9.1.2.5.1.1. Os “Agentes Públicos” podem ser utilizados em um cenário Intra Cloud Pública em que a PREFEITURA deseja monitor o desempenho ou a disponibilidade de um determinado ativo, entre regiões e/ou zonas de disponibilidade de um Provedor de Cloud Pública;

9.1.2.5.1.2. Os “Agentes Públicos” podem ser utilizados para monitorar ativos de um Provedor de Cloud Pública, a partir da infraestrutura de um Provedor de Cloud Pública alternativo.

9.1.2.6. "Agentes Internos" deverão ser entidades baseadas em software disponíveis, no mínimo, nos seguintes formatos:

9.1.2.6.1. OVA/OVF;

9.1.2.6.2. Hiper-V;

9.1.2.6.3. Imagem ISO;

9.1.2.6.4. Imagem para Cisco IOS-XE;

9.1.2.6.5. Imagem para contêiner Juniper Junos;

9.1.2.6.6. Pacote Linux;

9.1.2.6.7. Contêiner do Docker;

9.1.2.6.8. Imagem para Raspberry Pi;

9.1.2.6.9. Modelo para AWS CloudFormation.

9.1.2.7. Deve ser possível a utilização de "Agentes Internos" para monitorização/testes de dentro para fora. Este descreve o cenário em que o usuário final do aplicativo é a equipe da PREFEITURA. O aplicativo pode ser hospedado em IaaS, uma AWS VPC, por exemplo, ou ser baseado em SaaS. De qualquer forma, a comunidade de usuários está dentro e o serviço monitorado está fora da empresa.

9.1.2.8. O "Agente de Usuário Final" deve assegurar a experiência digital do usuário final, independentemente de onde o usuário esteja localizado, onde o aplicativo está hospedado e sem levar em conta os limites administrativos entre eles;

9.1.2.9. O "Agente de Usuário Final" deve ser um software a ser instalado em estações de trabalho do usuário final, com ambiente operacional Microsoft Windows ou Apple Mac;

9.1.2.10. O "Agente de Usuário Final" deve trabalhar em conjunto com os browsers Internet Explorer ou Google Chrome para fornecer visibilidade do dispositivo do usuário real;

9.1.2.11. O "Agente de Usuário Final" deverá possibilitar o monitoramento de usuários nômades, ou usuários que trabalham em home office através de uma conexão com a Internet. O “Agente de Usuário Final” deve identificar, no mínimo, os seguintes problemas do ponto de vista do usuário final:

9.1.2.11.1. Problema de conectividade do usuário à Internet, seja via WiFi, ou rede cabeada;

9.1.2.11.2. Problema com o Internet Service Provider (ISP) que atende à conectividade Internet do usuário final;

9.1.2.11.3. Problema com o provedor de serviço SaaS sendo acessado pelo usuário;

9.1.2.11.4. Problema ocorrendo em salto de rotemanete na Internet.

9.1.2.12. Além dos testes regulares, o "Agente de Usuário Final" deve suportar a capacidade de monitorar o tráfego real do usuário e derivar estatísticas da experiência do usuário a partir desse tráfego observado.

9.1.3. **Requisitos Gerais dos Testes:**

9.1.3.1. Os testes realizados a partir de sites e redes internas deverão conter, no mínimo, as seguintes informações:

9.1.3.1.1. Nome do nó/salto L3 na rede;

9.1.3.1.2. Endereço IP;

9.1.3.1.3. Prefixo;

9.1.3.1.4. Labes MPLS (se houver);

9.1.3.1.5. Tempo de conexão salto-a-salto;

9.1.3.1.6. Latência;

9.1.3.1.7. Jitter;

9.1.3.1.8. MTU;

9.1.3.1.9. Cada salto L3 que transitou durante a conexão;

9.1.3.1.10. Cada link que transitou durante a conexão.

9.1.3.2. A solução ofertada deverá ter a capacidade de fornecer informações para avaliar o desempenho da rede entre dois sites físicos, ter métricas de throughput bidirecional e medição de métricas de conectividade entre diferentes sites da PREFEITURA. Os testes necessários para comprovar o desempenho da conectividade devem ser executados entre os sites.

9.1.3.3. Os testes de sites internos poderão ser realizados em direção a um site de destino, definido como um endereço IP ou como um nome de host. Esses testes devem ser capazes de fornecer informações de parâmetros em uma direção ou em ambas as direções, ou seja, métricas de onde os testes são realizados para o servidor de destino e vice-versa, quando o destino é um servidor de um sistema ou aplicativo de destino;

9.1.3.3.1. Os testes executados devem ser capazes de fornecer informações relacionadas ao desempenho da conectividade com o servidor ou serviço de destino, a partir dos sites definidos pela PREFEITURA.

9.1.3.4. Os testes realizados pela solução deverão possibilitar a visualização de, no mínimo, as seguintes informações:

9.1.3.4.1. Métricas de latência, oscilação e perda de pacotes no processo de conexão entre o site de origem e o servidor de destino;

9.1.3.4.2. Um mapa gráfico da rota seguida entre o site de origem e o servidor de destino, incluindo os diferentes saltos de conectividade, que podem ou não ser por meio de um link MPLS, uma conexão VPN e/ou pela Internet;

9.1.3.4.3. Validação da disponibilidade do servidor de destino;

9.1.3.4.4. Degradação da rede através da rota seguida. Esta degradação pode ser determinada de acordo com parâmetros definidos como níveis máximos aceitáveis;

9.1.3.4.5. Visibilidade do tráfego entre ISPs (Internet Service Providers).

9.1.3.5. A solução deve ser capaz de apresentar informações sobre a conectividade com um servidor HTTP a partir de um site de origem, seja de sites externos fornecidos pela PREFEITURA através da Internet, ou de sites internos. Os testes efetuados numa base programada devem fornecer, no mínimo, informações sobre:

9.1.3.5.1. Disponibilidade do servidor HTTP (porcentagem de tempo em que o site fica disponível);

9.1.3.5.2. Tempo de resposta entre o início da solicitação (antes da solicitação DNS) até que o cliente/origem receba a primeira parte da resposta do servidor de destino;

9.1.3.5.3. Taxa de transferência em MB/s.

9.1.3.6. A solução ofertada deve ser capaz de mostrar o tempo gasto para carregar uma página web de destino, sendo capaz de mostrar no console de exibição o tempo de carregamento de cada um dos elementos que compõem a página web de destino (exemplo: imagens, captchas, vídeos) a fim de identificar quais elementos são os que levam mais tempo ou causam tempos de carregamento excessivos na página;

9.1.3.7. A solução deve fornecer métricas sobre a disponibilidade do servidor HTTP, seu tempo de resposta e a taxa de transferência consumida ao executar o teste de validação;

9.1.3.8. Da mesma forma, de acordo com o acima mencionado, o teste deve ser capaz de fornecer as seguintes informações:

9.1.3.8.1. Tempo de resolução de nome e domínio (DNS);

9.1.3.8.2. Tempo gasto para a carregar cada objeto;

9.1.3.8.3. Tempo necessário para se conectar ao servidor;

9.1.3.8.4. Tempo necessário para transferir cada objeto do servidor para o navegador;

9.1.3.8.5. Se um objeto foi bloqueado ou não.

9.1.3.9. A solução deve ter a capacidade de simular transações na aplicação web de destino, executando as etapas exigidas pela PREFEITURA. A solução utilizada para a simulação de transações deve ter a capacidade de executar um código Javascript com as etapas necessárias para obter informações sobre os tempos de execução das diferentes etapas das transações;

9.1.3.10. A execução da simulação das transações deverá poder ser realizada a partir de pontos internos nas dependências da PREFEITURA ou, a partir de, no mínimo, 2 (dois) sites externos no território Nacional e, de pelo menos 200 (duzentos) sites internacionais através da Internet;

9.1.3.11. A solução proposta deve ter a capacidade de fornecer visibilidade sobre a porcentagem de utilização da CPU, porcentagem de utilização de memória RAM, desempenho da rede WiFi ou cabeada a qual está se conectando, o status da VPN, com mínima invasão, sem afetar o desempenho dos dispositivos e garantindo total privacidade e segurança das informações;

9.1.3.12. O agente implantado para obter a Experiência do Usuário Final descrita acima deve ser capaz de fornecer informações sobre a experiência de navegação do usuário ao visitar um domínio estabelecido;

9.1.3.13. A solução deve disponibilizar múltiplos tipos de testes, devendo a PREFEITURA ter a opção de selecionar um ou mais testes adequados à aplicação ou ativo que deseja testar/monitorar;

9.1.3.14. É obrigatório que os testes sejam sintéticos, sendo projetados para a geração de tráfego na rede que se assemelha ao tráfego real do usuário;

9.1.3.14.1. Não será aceita solução que utilize a amostragem de fluxos e/ou a captura de pacotes, garantindo dessa forma a privacidade dos dados.

9.1.3.15. Os testes deverão ser definidos pelo administrador da PREFEITURA utilizando a plataforma da solução disponível em nuvem. A plataforma da solução deverá ser responsável por distribuir os parâmetros de teste configurados para os agentes aplicáveis selecionados. Os agentes deverão executar os testes na frequência configurada. Os agentes deverão consolidar os dados de resultados, encaminhando os mesmos para a plataforma da solução;

9.1.3.16. Após o recebimento dos resultados, a plataforma da solução deve processar os dados, realizar a correlação entre os diferentes componentes individuais do teste e disponibilizar esses dados por meio do aplicativo web da solução e da API da solução em tempo real;

9.1.3.16.1. Os resultados dos testes devem ser alimentados na infraestrutura de alerta e notificação da solução.

9.1.3.17. A solução deve ser capaz de executar testes no formato “tests nest”, onde vários testes são agrupados, fazendo com que os testes de camada alta incluem implicitamente testes de nível inferior, por exemplo, um teste de “page load” web inclui implicitamente o teste do servidor HTTP, o teste de rede e o monitoramento BGP;

9.1.3.18. A solução ofertada deverá suportar a correlação dos resultados dos testes na linha do tempo. Quando os resultados do teste de “page load” web são exibidos, os dados dos outros testes também devem ser incluídos. Os resultados são correlacionados no domínio do tempo para o usuário, tornando a navegação

trivial para cima e para baixo na pilha de teste, ao mesmo tempo em que se move para frente e para trás no tempo.

9.1.4. **Tipos de Testes e Requisitos:**

9.1.4.1. A solução ofertada deverá disponibilizar, no mínimo, os seguintes Testes de Camada 3:

9.1.4.1.1. **Teste de Monitoramento BGP**

9.1.4.1.1.1. O teste de Monitoramento BGP deve monitorar a disponibilidade de prefixos públicos na Internet. A solução deverá coletar os dados usando mecanismos internos, como acessar informações do Route Views Project (routeviews.org) da Universidade de Oregon;

9.1.4.1.1.2. Os dados do BGP devem ser coletados de dezenas de monitores públicos em todo o mundo. Esses dados devem ser usados para produzir uma Visualização de Rota BGP que exibe um sistema autônomo pela visualização autônoma do caminho de cada monitor para o prefixo de destino;

9.1.4.1.1.3. As métricas coletadas e apresentadas devem incluir, no mínimo:

9.1.4.1.1.4. Mudanças de caminho: O número de mudanças de caminho AS durante a jornada de teste. Uma rota retirada e reanunciada deve ser considerada conta duas alterações. Picos grandes ou frequentes devem indicar instabilidade de rota;

9.1.4.1.1.5. Acessibilidade: Porcentagem de tempo durante a jornada de teste para a qual o monitor tinha uma rota para o prefixo monitorado. Acessibilidade inferior a 100% deve indicar um problema de roteamento ou, o caminho para o destino, para o monitor, está disponível por meio de outro prefixo.

9.1.4.1.1.6. Atualizações: contagem das atualizações do BGP durante a rodada de testes.

9.1.4.1.1.7. Os testes BGP devem ter a opção de serem configurados para 'incluir prefixos cobertos', se um prefixo mais específico do que o especificado for anunciado. Os dados para o prefixo mais específico também deverão ser coletados.

9.1.4.1.1.8. Além de monitorar a acessibilidade do prefixo público, a solução deve fornecer a opção de fazer peer com uma empresa para fornecer visibilidade BGP de dentro do agente instalado na PREFEITURA, para um prefixo de escolha do PREFEITURA.

9.1.4.1.2. **Teste de rede**

9.1.4.1.2.1. Os testes de rede devem oferecer opções flexíveis. A solução deve suportar testes de rede 'Agente para Servidor' e 'Agente para Agente'. Embora o termo 'servidor' seja utilizado, a solução deve ser flexível para permitir que o administrador configure qualquer nó IP como o destino de um teste de agente para servidor.

9.1.4.1.2.2. No caso de testes de ‘Agente para Servidor’, a solução deve suportar a utilização dos protocolos TCP e ICMP;

9.1.4.1.2.3. No caso de testes ‘Agente para Agente’, a solução deve suportar a utilização dos protocolos TCP ou UDP;

9.1.4.1.2.4. Em cada caso, a configuração mínima necessária é o IP de destino ou FQDN, e uma seleção dos agentes disponíveis. A lista de agentes deve incluir "Agentes Internos" e "Agentes Públicos" associados à conta do cliente;

9.1.4.1.2.5. O teste 'Agente para Agente' deve suportar testes bidirecionais. Ou seja, ambos os agentes em um par podem originar dados de teste;

.1.4.1.2.5.1. A opção de teste bidirecional 'Agente para Agente' deve estar disponível como opção para descobrir problemas no caminho inverso, isto é assimetria de roteamento.

9.1.4.1.2.6. Os testes de rede devem ter a flexibilidade de serem configurados para serem executados em intervalos de tempo entre um minuto e uma hora;

9.1.4.1.2.7. O teste de rede deve reunir métricas de ponta a ponta e métricas por salto. As métricas devem incluir, no mínimo:

.1.4.1.2.7.1. Para cada agente, e cada salto, latência, perda e estatísticas de jitter devem ser registrados para cada rodada de teste, juntamente com quaisquer regravações de DSCP;

.1.4.1.2.7.2. O administrador pode exibi-los em forma de resumo para todos os agentes, um subconjunto de agentes ou em uma base de agente individual;

.1.4.1.2.7.3. Os dados devem ser exibidos em forma tabular ou por meio de visualização de caminho, onde cada agente e cada salto do agente para o destino é mostrado graficamente;

.1.4.1.2.7.4. Além disso, o administrador deve ser capaz de filtrar e colorir a visualização com base em critérios definidos pelo usuário, como latência, perda de pacotes ou regravações de ponto de código;

.1.4.1.2.7.5. Os caminhos podem ser mostrados com ou sem endereço IP, localização física, detalhes do AS ou tipo de interface;

.1.4.1.2.7.6. Todos os dados devem ter a opção de serem mostrados durante a navegação para frente e para trás na linha do tempo;

.1.4.1.2.7.7. Por padrão, um teste de rede deve incluir um teste BGP para o prefixo que abrange o endereço IP do dispositivo de destino.

9.1.4.1.3. **Teste do servidor HTTP**

9.1.4.1.3.1. Os Testes de Camada Web devem consistir em testes que obtenham progressivamente mais detalhes. Esses testes devem se aplicar principalmente a servidores Web de aplicativos, mas também podem ser usados para testar pontos de extremidade de API. Os destinos de teste podem ser acessíveis publicamente ou internos a redes e domínios internos da PREFEITURA;

9.1.4.1.3.2. O teste deve medir a disponibilidade e o desempenho de um serviço HTTP. O teste deve incluir, no mínimo, as seguintes séries de fases:

.1.4.1.3.2.1. DNS: A parte de domínio da URL de destino de teste é resolvida para um endereço IP;

.1.4.1.3.2.2. Conexão: Um handshake TCP de 3 (três) vias é executado;

.1.4.1.3.2.3. SSL: Os mecanismos de segurança são negociados;

.1.4.1.3.2.4. Envio: Uma solicitação HTTP é enviada;

.1.4.1.3.2.5. Recebimento: Uma resposta HTTP é aguardada e recebida;

.1.4.1.3.2.6. HTTP: O código de resposta HTTP é validado;

.1.4.1.3.2.7. Verificação de conteúdo: A verificação do conteúdo recebido é realizada comparando-o com uma expressão regular.

9.1.4.1.3.3. O teste deve ser altamente configurável para atender às necessidades individuais. Vários esquemas de autenticação devem ser suportados, além de cabeçalhos personalizados e opções SSL;

9.1.4.1.3.4. Os casos de uso para este teste devem incluir: alerta sobre problemas de disponibilidade ou desempenho do serviço, detectar problemas em serviços baseados em anycast ou GLBS, validar o desempenho e roteamento da CDN;

9.1.4.1.3.5. O teste deverá apresentar status por resumo de fases, para que possa ser verificado a desambiguação entre problemas de servidor versus rede;

9.1.4.1.3.6. Este teste deve ter a opção de ser configurado para ser executado em uma frequência entre um minuto e uma hora;

9.1.4.1.3.7. Além das informações da fase de conexão, o teste do Servidor HTTP deve registrar a disponibilidade mínima, o tempo de resposta e a taxa de transferência para cada ciclo de teste;

9.1.4.1.3.8. Por padrão, um teste de servidor HTTP deve incluir os testes de rede subjacente e BGP.

9.1.4.1.4. **Teste de “Page Load” HTTP**

9.1.4.1.4.1. O teste de “page load” http deve ser criado no teste do servidor HTTP adicionando métricas de desempenho no navegador;

9.1.4.1.4.2. As métricas devem incluir o tempo de carregamento da página concluída e as informações de fase para cada componente DOM na página apresentada em formato cascata. Essas informações devem ser geradas por cada agente que executa o teste;

9.1.4.1.4.3. Além do diagrama em cascata, as informações dos componentes devem ser resumidas por provedor de origem, permitindo pronta comparação entre provedores que contribuem com conteúdo para a página;

9.1.4.1.4.4. Os testes instantâneos de “page load” http devem fornecer uma captura de tela após a conclusão do teste, enquanto os testes de “page load” http agendados devem fornecer capturas de tela quando os erros são gravados;

9.1.4.1.4.5. Os casos de uso deste teste devem incluir: identificar objetos que impeçam ou prolonguem a conclusão do carregamento da página, monitorar o desempenho entre provedores de conteúdo, bem como, fornecer as métricas descritas em relação à experiência no navegador;

9.1.4.1.4.6. Os testes de “page load” http também devem incorporar testes de servidor HTTP, rede e BGP;

9.1.4.1.4.7. Este teste deve ter a opção de ser configurado para ser executado em uma frequência entre um minuto e uma hora.

9.1.4.1.5. **Teste de Transação Web**

9.1.4.1.5.1. Os testes de transação web devem ser baseados no teste de ”page load” e, portanto, incluir também os dados de teste HTTP, rede e BGP;

9.1.4.1.5.2. Os testes de transação web devem imitar a interação do usuário com um site por meio de testes com script. Os scripts podem ser derivados de uma função "Gravador", este software captura e registra as ações de um usuário à medida que um site é navegado e gera um script que pode ser importado diretamente para a definição de Teste de Transação;

9.1.4.1.5.3. O administrador deve ter a opção de modificar o script conforme necessário, adicionando marcadores de temporização opcionais para medir o tempo de execução de várias fases de uma transação e capturas de tela, onde quer que elas sejam desejadas na transação;

9.1.4.1.6. **Teste SIP**

9.1.4.1.6.1. Testes da camada de voz devem abranger a conectividade do plano de controle (SIP) e do plano de dados (RTP);

9.1.4.1.6.2. Este teste deve reunir resultados de testes de camada de rede, resultados de BGP e medições orientadas pelo Protocolo de Iniciação de Sessão (SIP);

9.1.4.1.6.3. No lado do protocolo SIP, o teste deve monitorar a disponibilidade do servidor SIP e o tempo de resposta. O teste deverá verificar a disponibilidade do serviço por meio de uma solicitação SIP OPTIONS, o chamado ping SIP.

9.1.4.1.7. **Teste RTP**

9.1.4.1.7.1. Um teste de fluxo RTP (Real-time Transport Protocol) deve criar um fluxo de dados de voz simulado entre dois Agentes da solução atuando como agentes de usuário VoIP;

9.1.4.1.7.2. Os pacotes RTP devem ser enviados entre um ou mais Agentes e um Agente de destino e, usar o UDP como protocolo de transporte para obter métricas de Pontuação de Opinião Média (MOS), perda de pacotes, descartes, latência e Variação de Atraso de Pacotes (PDV);

9.1.4.1.7.3. As métricas produzidas são unidirecionais (da origem ao destino). O teste RTP Stream deve fornecer a porta do servidor, a duração da chamada, o tamanho do buffer de de-jitter e as opções de configuração do codec;

9.1.4.1.7.4. O teste RTP deve incluir os testes de rede subjacente e BGP.

9.1.4.1.8. **Teste de Servidor DNS**

9.1.4.1.8.1. O teste de Servidor DNS deve alertar sobre mapeamento de registro DNS incorreto, medir o desempenho do servidor de nomes e a disponibilidade, verificar o desempenho do GSLB & GeoDNS;

9.1.4.1.8.2. Os testes de Servidor DNS devem consultar os servidores de nomes autoritativos de cada local, mostrando disponibilidade e tempo de resolução por local. Além dessas métricas, a rede subjacente e os testes BGP também devem ser incluídos em um teste de servidor DNS.

9.1.4.1.9. **Teste de DNS Trace**

9.1.4.1.9.1. O teste de DNS Trace deve verificar a delegação de registros DNS entre zonas pai e filho, conforme esperado. O teste deve mostrar a hierarquia DNS de um domínio de destino a partir de vários pontos de vista;

9.1.4.1.9.2. O teste de DNS Trace deve rastrear a disponibilidade de uma resolução e o tempo final de consulta para atingir a resolução por ponto de vantagem e a média geral.

9.1.4.1.10. **Teste DNSSEC**

9.1.4.1.10.1. O teste DNSSEC deve verificar a assinatura digital dos registros de recursos DNS que compreendem toda a cadeia e, portanto, valida a autenticidade dos registros de recursos de acordo com as Extensões de Segurança do Sistema de Nomes de Domínio. O teste deve produzir uma condição de aprovação ou reprovação para cada ponto de vantagem testado.

9.1.4.2. **Testes específicos do tipo "Experiência do Usuário Final":**

9.1.4.2.1. A solução deve suportar testes específicos do tipo "Experiência do Usuário Final". Nesse caso, um agente específico deve ser implantado na estação de trabalho do usuário final;

9.1.4.2.2. Fazendo parte do resultado da “Experiência do Usuário Final”, deve ser possível monitorar as interações do usuário com sites de interesse, com base nas sessões do navegador;

9.1.4.2.3. Também deve realizar testes agendados baseado na web e testes de nível de rede.

9.1.4.2.4. **Monitoramento de Sessão do Navegador**

9.1.4.2.4.1. O monitoramento da sessão do navegador deve coletar dados da experiência do usuário final para sites de interesse. O agente, nesse caso, deve relatar no mínimo o tempo de resposta do servidor, o tempo de carregamento da página, os redirecionamentos e quaisquer erros encontrados. Ele também deverá capturar informações em cascata;

9.1.4.2.4.2. Enquanto as sessões do navegador estiverem em execução, o deverá registrar dados de desempenho da camada de acesso à rede paralela. A camada de acesso à rede deve registrar, no mínimo, o desempenho das conexões físicas, com ou sem fio do Usuário Final, gateways, VPNs, proxies e servidores DNS. Os dados de caminho também devem ser capturados e apresentados em uma exibição de visualização de caminho;

9.1.4.2.4.3. Vários dados de "Experiência do Usuário Final" devem ser exibidos simultaneamente, de forma agregada, ou filtros podem ser definidos em uma variedade de critérios para restringir a exibição a um subconjunto ou a um agente individual. Os critérios de filtro devem incluir características do ponto de extremidade, do usuário, do site visitado ou do rótulo;

9.1.4.2.4.4. O controle sobre os dados capturados é importante. É provável que o administrador esteja interessado apenas no desempenho dos sites usados na gestão do negócio, para esse fim

9.1.4.2.4.5. O administrador da solução deve ser capaz de definir uma ou mais listas de 'domínio monitorado'. Cada lista deve especificar um ou mais nomes de domínio totalmente qualificados com caminho de URL opcional anexado. Sempre que o usuário visitar um site correspondente à lista de domínios monitorados, as estatísticas deverão ser capturadas. O administrador poderá filtrar "ruídos" não relacionados ao negócio prontamente;

9.1.4.2.4.6. O administrador da solução deve ser capaz de definir 'redes monitoradas', onde o usuário deve estar conectado a uma rede monitorada antes que as estatísticas de sessão do navegador sejam geradas. As redes monitoradas devem ser especificadas como um endereço IP ou intervalo de endereços IP. O administrador poderá coletar dados de desempenho quando um usuário está conectado a partir de um intervalo de endereços corporativos e ignorar todas as outras conexões, se desejar;

9.1.4.2.5. **Agendamento de Testes**

9.1.4.2.5.1. A solução deve oferecer suporte a testes HTTP e testes de Agente para Servidor, agendados. Esses testes devem ser executados sem a interação do usuário final;

9.1.4.2.5.2. A solução deve apresentar formas de agrupar ou organizar os agentes e também os testes, para facilitar a associação ou a combinação entre os agentes e os testes;

9.1.4.2.5.3. A solução deverá apresentar opções de configuração de frequência para a realização dos testes.

9.1.5. **Requisitos de Consumo de Dados:**

9.1.5.1. **Dashboards ou Painéis**

9.1.5.2. Os painéis devem mostrar dados próximo ao tempo real. Eles devem ser altamente configuráveis pelo usuário para exibir dados pertinentes ao caso de uso desse usuário. Os painéis devem ser construídos por meio da combinação de widgets personalizáveis em uma visualização desejada pelo usuário;

9.1.5.3. Os widgets devem exibir os dados dos resultados do teste de várias maneiras diferentes. No mínimo, a solução deve ter os tipos de widget definidos nas tabelas a seguir:

| Tipos de Recursos | Descrição |
|---|---|
| Lista de Alertas | Checar os alertas que estavam ativos durante o período configurado |
| Testes | Uma exibição ao vivo de 12 (doze) horas com uma lista de testes configurados em seu grupo de contas para uma visão geral da integridade do teste de alto nível. Testes desativados devem ser destacados visualmente. |
| Status do Agente | Uma visão em tempo real do status da empresa e dos agentes de usuário final, para se ter uma ideia da integridade geral do agente. |

| Tipos de Recursos | Descrição |
|---|---|
| Gráfico de Barra Empilhada | Deve apresentar barras horizontais de histograma com vários valores, úteis para dados de métricas compostas (como resposta HTTP ou tempo de busca) e, para comparar valores entre vários testes ou comparar valores por país. As barras podem ser orientadas horizontalmente ou verticalmente como colunas. |
| Gráfico de Barra Agrupada | Deve representar vários valores como barras individuais em um grupo de barras. As barras podem ser orientadas horizontal ou verticalmente como colunas. |
| Gráfico Circular (Pizza) | Semelhante aos recursos de gráfico de barras empilhadas, deve representar vários valores como segmentos de pizza de tamanho proporcional. |

| Tipos de Recursos | Status |
|---|---|
| Tabela | Deve permitir uma divisão de números por linhas e colunas. Tanto as linhas quanto as colunas podem ser listadas por teste, país, continente ou fonte de dados ou o agregado desses. |
| Tabela Multi-Métrica | Devem apresentar colunas com métricas diferentes, em vez de uma única métrica para a tabela inteira. |
| Números | Um ou mais cartões, onde cada cartão deve exibir uma única quantidade escalar, como uma média de pacotes perdidos ou tempos de carregamento de páginas, ou uma série de alertas. |

| | |
|---|---|
| Grade de Cores | Deve exibir uma matriz de cartões coloridos, onde a cor de cada cartão depende da escala de cores configurada para erros ou desempenho insatisfatório do teste alvo, bom desempenho do teste e vários níveis de degradação. |

| Tipos de Recursos | Status |
|---|---|
| Linha | Deve apresentar gráficos de linhas com o tempo no eixo horizontal e a quantidade selecionada no eixo vertical. |
| Área Empilhada | Gráficos de linhas com o tempo no eixo horizontal e as quantidades selecionadas no eixo vertical. Eles devem ser utilizados de forma semelhante aos gráficos de barras empilhadas, mas mostrando valores ao longo do tempo. |
| Diagrama de Caixas | Exibição dos valores dos dados versus o tempo no eixo horizontal, com o eixo vertical exibindo a mediana, os pontos de dados mínimos e máximos por valor de tempo. |

| Tipos de Recursos | Status |
|---|---|
| Mapa | Deve exibir dados em um mapa mundial, com base na localização dos sistemas de teste. Os dados devem ser exibidos por país, por continentes e por agente. |

9.1.5.4. Devem estar disponíveis para utilização, no mínimo, os seguintes painéis típicos:

9.1.5.4.1. Painel SaaS global, para uma empresa fortemente dependente de provedores de SaaS;

9.1.5.4.2. Painel SD-WAN, mostrando o desempenho comparativo da sobreposição da empresa versus a subposição;

9.1.5.4.3. Painel UCaaS, mostrando o desempenho de provedores de tronco Webex e SIP em uma região ou globalmente;

9.1.5.4.4. Painel do Office 365, mostrando o desempenho com base geográfica para diferentes componentes do O365.

9.1.5.5. Os painéis devem mostrar uma visão global consolidada da integridade da experiência do usuário, bem como as principais dependências para oferecer uma ótima experiência do usuário, quebrando silos em toda a empresa e provedores externos;

9.1.5.6. A solução deve oferecer uma série de painéis pré-configurados, que poderão ser utilizados da forma como estão ou, duplicar os painéis internos e, em seguida, modificá-los.

9.1.5.7. **Relatórios**

9.1.5.7.1. Os relatórios devem ser semelhantes aos painéis, em termos de flexibilidade e como eles são construídos, usando widgets de relatório. Os relatórios devem estar disponíveis e ser gerados sob demanda ou de forma programada;

9.1.5.7.2. Os relatórios devem ter a opção de ser enviados automaticamente via e-mail;

9.1.5.7.3. Os relatórios devem capturar dados em um determinado momento do tempo (point-in-time), e ao longo de um intervalo de tempo especificado na definição do mesmo;

9.1.5.7.4. Os relatórios devem ser capazes de mostrar dados de tendência, ao longo de um dia, semana ou mais;

9.1.5.7.5. A solução deve ter disponíveis, por padrão, alguns relatórios internos fornecidos como ponto de partida com base nos tipos de teste definidos;

9.1.5.7.6. Os relatórios podem ser usados para reter dados históricos além do período de retenção de dados da solução;

9.1.5.7.7. A solução ofertada deve ter a capacidade de gerar relatórios sob demanda e programados. Os dados gerados por esses relatórios devem poder ser apresentados, no mínimo, por meio de gráficos, dados numéricos e tabelas. Os relatórios devem poder ser enviados de forma programada para outros usuários por e-mail;

9.1.5.7.8. A configuração dos relatórios deve ser possível através de widgets que permitam ao usuário criar diferentes modelos com os parâmetros correspondentes para serem exibidos da maneira mais conveniente para o usuário.

9.1.5.8. **Alertas**

9.1.5.8.1. A solução ofertada deve ter a capacidade de alertar, proativamente, caso durante a execução dos testes, ocorra um evento de interesse. Esses alertas devem poder ser enviados por e-mail e webhooks;

9.1.5.8.2. A solução deve suportar a integração dos alertas em plataformas de terceiros;

9.1.5.8.3. Quando um teste é criado, uma regra de alerta associada também deve ser criada, usando um critério padrão;

9.1.5.8.4. A solução deve permitir que o responsável pelo teste revise os critérios de alertas e os configure para se adequar ao seu caso de uso, evitando a criação de alertas desnecessários, sem que sejam perdidos eventos críticos;

9.1.5.8.5. Os alertas devem ser suficientemente flexíveis para permitir a definição de uma condição de erro com base em numerosos critérios extraídos de métricas pertinentes ao tipo de teste;

9.1.5.8.6. Devem ser permitidos vários critérios por alerta, sendo um ou todos necessários para disparar o alerta;

9.1.5.8.7. Os alertas devem ser configurados para disparar quando uma condição de erro afirmar, para N ciclos de testes sucessivos, em que N ≥ 1, isso pode ser correspondido a um número mínimo de agentes que precisam observar o erro em uma rodada de teste antes que um alerta seja acionado;

9.1.5.8.8. Quando um alerta é disparado, a notificação deve assumir várias formas (ações). A ação mais simples deve ser um e-mail, onde a caixa de correio do destinatário não precisa ser uma solução associada ao usuário/caixa de correio, permitindo o recebimento para um alias de remetente, por exemplo;

9.1.5.8.9. A solução deve ter a capacidade de definir, com antecedência, uma janela de supressão de alertas. Durante o tempo definido, os testes selecionados deverão ter os alertas suprimidos, permitindo que falsos positivos sejam suprimidos durante janelas de manutenção conhecidas;

9.1.5.8.10. As janelas de supressão de alertas disponíveis devem ser únicas ou configuradas para se repetirem regularmente;

9.1.5.8.11. A plataforma da solução deve suportar a integração no Slack, PagerDuty e ServiceNow;

9.1.5.8.12. A plataforma da solução deve suportar a integração via webhooks, garantindo alternativas de integração mais flexíveis com outros sistemas.

9.1.5.9. **Compartilhamento de Dados de Teste**

9.1.5.9.1. A solução ofertada deve fornecer os meios para compartilhar dados, independentemente do destinatário possuir ou não a plataforma;

9.1.5.9.2. Devem ser fornecidos, no mínimo, os seguintes métodos de compartilhamento de dados:

9.1.5.9.2.1. Para os destinatários que utilizam a mesma plataforma, os testes devem ser compartilhados via modo instantâneo, onde a é feita captura de todos os dados do teste em torno de um ponto no tempo;

9.1.5.9.2.2. Para os destinatários usuários externos, que não utilizam a mesma plataforma, o compartilhamento deve ser feito através do modo 'snapshot', onde uma URL exclusiva é gerada para ser compartilhada.

9.1.5.9.2.3. Ao acessar o link de snapshot, o destinatário deverá ter a mesma exibição de teste baseada na Web que o usuário da solução, juntamente com a capacidade de navegar para frente e para trás, na linha do tempo e, para cima e para baixo na pilha de teste;

9.1.5.9.2.4. O destinatário não precisará ser um usuário da plataforma e não precisará se cadastrar na plataforma da solução para ter acesso às informações.

9.1.5.10. **Requisitos de API da Plataforma**

9.1.5.10.1. A solução ofertada deverá possuir uma GUI baseada na Web para acesso às informações, além de disponibilizar uma API para integração com outros sistemas;

9.1.5.10.2. A API deve ser aberta, em formato RESTful e, deve estar disponível para a comunidade de desenvolvedores para facilitar a integração com sistemas, soluções e aplicativos de terceiros;

9.1.5.10.3. A documentação e as especificações da API deverão ser fornecidas pela empresa CONTRATADA;

9.1.5.10.4. A API deverá possibilitar, no mínimo, os seguintes usos:

9.1.5.10.4.1. Integração com sistemas de alertas externos;

9.1.5.10.4.2. Integração com sistemas de relatórios externos;

9.1.5.10.4.3. Integração com soluções complementares, como sistemas APM;

9.1.5.10.4.4. Integração com sistemas de provisionamento e faturamento MSP;

9.1.5.10.4.5. Acesso a dados para relatórios personalizados;

9.1.5.10.4.6. Administração em massa de usuários;

9.1.5.10.4.7. Administração em massa de configurações de teste.

9.1.5.11. **Requisitos de Administração da Plataforma**

9.1.5.11.1. A solução ofertada deverá suportar um modelo RBAC (Role-Based Access Control) para gerenciamento de usuários e grupos;

9.1.5.11.2. A solução deverá implementar Organizações e Grupos de Contas Associados. Cada cliente deverá ser mapeado para uma Organização. Uma Organização deve conter um ou mais grupos de contas;

9.1.5.11.3. Deve estar disponível para os clientes a capacidade de provisionar e usar vários grupos de contas para dividir sua organização entre unidades de negócios separadas, equipes, equipes de aplicativos e assim

por diante;

9.1.5.11.4. Deve ser possível a configuração dos usuários em, no mínimo, três funções predefinidas, podendo estas funções ser modificadas e funções adicionais criadas;

9.1.5.11.5. A solução deverá possibilitar a configuração de um Administrador Organizacional, responsável por executar tarefas administrativas em toda a organização. As tarefas devem incluir a administração de agentes, testes, painéis e relatórios;

9.1.5.11.6. A solução deverá possibilitar a criação de um Administrador de Conta, com direitos semelhantes aos do administrador organizacional, porém, apenas dentro de um ou mais grupos de contas aos quais tenha sido associado sob a organização;

9.1.5.11.7. A solução deve suportar logon único via SAML e provisionamento de usuários via SCIM, permitindo, por meio de sua API, provisionar e desprovisionar usuários com base nas propriedades do Provedor de Identidade;

9.1.5.11.8. A solução deve permitir que um usuário possa ter direitos entre grupos de contas dentro de uma organização;

9.1.5.11.9. Deverá permitir que os testes sejam compartilhados e que, o destinatário do compartilhamento não possa alterar os parâmetros de teste, que são somente leitura, no entanto, eles poderão definir regras de alerta independentes daquelas definidas no grupo de contas de compartilhamento;

9.1.5.11.10. O acesso aos dados relativos à medição através da GUI deve ser possível durante, pelo menos, 30 (trinta) dias. Esses dados também devem ser acessados via API da plataforma por pelo menos 90 (noventa) dias. Todas as contas de usuário, alertas, relatórios e testes configurados pelos clientes devem permanecer online enquanto a conta estiver ativa.

9.1.5.12. **Requisitos de Segurança**

9.1.5.12.1. A solução deverá cumprir, no mínimo, as seguintes Declarações de Privacidade e Certificações:

9.1.5.12.1.1. Declaração de privacidade do visitante do site;

9.1.5.12.1.2. Declaração de privacidade do usuário da plataforma;

9.1.5.12.1.3. Certificação Privacy Shield;

9.1.5.12.1.4. Framework Privacy Shield;

9.1.5.12.1.5. ISO/IEC 27001:2013;

9.1.5.12.1.6. Regulamentos da FTC;

9.1.5.12.1.7. Requisitos do Bureau of Industry and Security do Departamento de Comércio dos EUA;

9.1.5.12.1.8. Seja membro da Cloud Security Alliance (CSA)

9.1.5.12.1.9. Requisitos do Programa de Privacidade da TRUSTe

9.1.5.13. **Licenciamento da Solução**

9.1.5.13.1. Deverão ser ofertadas todas as licenças para utilização da solução ofertada, em quantidade suficiente para atender a todas as funcionalidades especificadas, além, de atender, no mínimo:

9.1.5.13.1.1. A utilização de 100 (cem) “Agentes de Usuário Final”, para estações de trabalho (end user);

9.1.5.13.1.2. A execução dos testes com origem em um “agentes interno” para, no mínimo, os seguintes casos de uso da PREFEITURA, proporcionando visibilidade sobre a experiência digital:

9.1.5.13.1.3. Aplicação internas utilizadas por servidores;

9.1.5.13.2. A execução dos testes com origem em um “agente público/externos”, no mínimo, os seguintes casos de uso da PREFEITURA, proporcionando visibilidade sobre a experiência digital:

9.1.5.13.2.1. Aplicações internas utilizadas por contribuintes;

9.1.5.13.2.2. Aplicação internas utilizadas por servidores.

9.1.5.13.3. Detalhes sobre os testes pretendidos utilizando agentes internos e público/externos, para os casos de usos citados nos itens anteriores:

| Finalidade | Testes | Qtde de Agentes Internos | Qtde de Agentes Externos | Qtde de Testes | Recorrência (minutos) | Timeout (segundos) |
|---|---|---|---|---|---|---|
| Testes sobre disponibilidade e performance de aplicações | Agent-to-Sever (Web Page Load, Web HTTP Server) | 1 | - | 4 | 5 | 10 (Page Load)<br><br>5 (HTTP Server) |
| Testes de DNS Server | Agent-to-Sever (DNS Server) | 1 | - | 4 | 5 | - |
| Acesso Aplicação Web | Agent-to-Sever (Web Transaction) | 1 | - | 4 | 5 | 30 |

9.1.5.14. O licenciamento da solução deverá ser ofertado no modelo de subscrição, incluindo o direito de utilização no modelo SaaS (Software as a Service) e os respectivos serviços de suporte técnico, pelo período de 48 (quarenta e oito) meses.

9.1.6. **Serviços de Implantação**

9.1.6.1. **Requisitos gerais**

9.1.6.1.1. O Serviço de Implantação visam possibilitar o início do uso efetivo da solução de Monitoramento de Experiencia Digital por meio da execução das configurações necessárias no software;

9.1.6.1.2. O Serviço de Implantação poderá ser executado de forma remota, desde que observados os procedimentos, as normas e as boas práticas de segurança para acesso remoto à infraestrutura de TI do PREFEITURA e utilizadas as soluções corporativas de comunicação e colaboração adotadas pelo PREFEITURA;

9.1.6.1.3. A arquitetura técnica adotada para implantação da solução de Monitoramento de Experiencia Digital deverá seguir as boas práticas recomendadas pelo fabricante visando desempenho, disponibilidade e segurança das informações.

9.1.6.2. **Vigência e prazos**

9.1.6.2.1. A CONTRATADA deverá iniciar a execução do Serviço de Implantação em até 15 (quinze) dias úteis após a disponibilização do software (entrega das subscrições/licenças) à PREFEITURA;

9.1.6.2.2. A CONTRATADA deverá apresentar um Plano de Implantação em até 30 (dez) dias úteis contados a

partir da assinatura do contrato;

9.1.6.2.3. O prazo máximo para execução do Serviço de Implantação será de 3 (três) meses contados a partir da assinatura do contrato;

9.1.6.2.4. Excepcionalmente, mediante justificativa da CONTRATADA, a PREFEITURA poderá prorrogar o prazo para início ou para conclusão do Serviço de Implantação ou para apresentação do Plano de Implantação;

9.1.6.2.5. A CONTRATADA comunicará a finalização do Serviço de Implantação à PREFEITURA que emitirá um Termo de Recebimento.

9.1.6.3. **Escopo**

9.1.6.3.1. No âmbito do Item Serviço de Implantação e Operação Assistida, a empresa contratada e a PREFEITURA terão responsabilidades conforme discriminado pelas seguintes fases:

9.1.6.3.1.1. Fase inicial;

9.1.6.3.1.2. Fase de definições;

9.1.6.3.1.3. Fase de construção do projeto;

9.1.6.3.1.4. Fase de implantação;

9.1.6.3.2. **Fase inicial;**

9.1.6.3.2.1. A CONTRATADA deverá prover o Gerenciamento de Projeto incluindo:

9.1.6.3.2.2. Coordenação de todas as atividades importantes do projeto;

9.1.6.3.2.3. Gerenciamento do escopo;

9.1.6.3.2.4. Gerenciamento de recursos;

9.1.6.3.2.5. Gerenciamento de riscos;

9.1.6.3.2.6. Alinhamento de contatos;

9.1.6.3.2.7. Cronograma de Projeto.

9.1.6.3.3. **Fase de definições;**

9.1.6.3.3.1. A CONTRATADA deverá realizar um levantamento de informações lógicas do ambiente atual

9.1.6.3.3.2. A PREFEITURA fornecerá os detalhes das aplicações existentes sobre as quais serão utilizadas como targets para a execução dos testes, tais como:

.1.6.3.3.2.1. Topologias lógicas;

.1.6.3.3.2.2. URLs;

.1.6.3.3.2.3. Endereço IP;

.1.6.3.3.2.4. Portas e protocolos;

.1.6.3.3.2.5. Servidores de DNS;

.1.6.3.3.2.6. Locais de instalação dos agentes;

.1.6.3.3.2.7. Políticas de segurança.

9.1.6.3.3.3. A CONTRATADA deverá prover uma matriz de compatibilidade para os agentes que serão instalados.

9.1.6.3.4. **Fase de construção do projeto;**

9.1.6.3.4.1. A PREFEITURA será responsável pela preparação de sites em produção sobre as seguintes

atividades:

9.1.6.3.4.2. Atualização de componentes e adequação do ambiente para que todos os elementos que compõem a solução estejam dentro da matriz de compatibilidade da solução ofertada;

9.1.6.3.4.3. Revisão de políticas de Firewalls, Proxys e similares, permitindo a comunicação através dos Agentes com plataforma SaaS da solução ofertada.

9.1.6.3.4.4. A PREFEITURA disponibilizará profissionais com conhecimentos sobre o ambiente e sobre as aplicações que serão utilizadas nos como targets dos testes, incluindo desenvolvedores, arquitetos de software, analistas de sistemas, administradores de redes e infraestrutura etc;

9.1.6.3.4.5. A CONTRATADA deverá criar os documentos HLD (High Level Design) e LLD (Low Level Design);

9.1.6.3.4.6. A PREFEITURA realizará a revisão e aprovação dos documentos HLD e LLD.

9.1.6.3.5. **Fase de implantação;**

9.1.6.3.5.1. A PREFEITURA fornrcerá as informações requisitadas para a realização do Setup Inicial;

9.1.6.3.5.2. A CONTRATADA deverá executar a implantação, conforme atividades a seguir:

.1.6.3.5.2.1. Setup Inicial da solução, incluindo Timezone, Usuários, Grupos e Roles;

.1.6.3.5.2.2. Apoio remoto na instalação de agentes;

.1.6.3.5.2.3. Para agentes internos e externos, configuração de até 20 (vinte) testes programados, além de criação de tags, labels ou grupos de agentes e de testes;

.1.6.3.5.2.4. Para agentes em estações de trabalho, configuração de até 10 (dez) teste programados, testes baseados em identificação de sessões no browser, deteção automática, além de criação de tags, labels ou grupos de agentes e de testes;

.1.6.3.5.2.5. Configuração de regras de alertas customizados baseadas nas métricas produzidas pelos testes;

.1.6.3.5.2.6. Elaboração de até 5 (cinco) dashboards ou painéis de visualização customizada dos resultados dos testes;

.1.6.3.5.2.7. Fine tunning de configurações em geral;

.1.6.3.5.2.8. Sessão de passagem de conhecimento.

9.1.6.3.5.3. A CONTRATADA deverá executar o Fine Tunning de configurações e a PREFEITURA trabalhará em conjunto com a CONTRATADA para chegar ao cenário desejado;

9.1.6.3.5.4. A CONTRATADA deverá apresentar uma Documentação Final do Projeto

9.1.7. **Serviços de Suporte Técnico**

9.1.7.1. A solução ofertada deverá possuir suporte técnico do fabricante, durante todo o período de vigência das licenças com, no mínimo:

9.1.7.1.1. Acesso aos serviços de suporte técnico, assistência técnica e solução de problemas do fabricante da solução, por telefone, ferramentas on-line e abertura de casos por plataformas web, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana – 24x7;

9.1.7.1.2. Acesso à base de conhecimentos, comunidades e ferramentas on-line da solução;

9.1.7.1.3. Patches, versões de manutenção, versões secundárias e versões principais do software da solução ofertada

## 10. SERVIÇO DE TREINAMENTO DAS SOLUÇÕES

10.1. A CONTRATADA deverá prestar serviços de Treinamentos para equipe da PREFEITURA conforme os conteúdos mínimos indicados a seguir com o intuito de assegurar a transferência de conhecimento:

10.2. O Treinamento não-oficial (ou repasse de conhecimento) deverá ser ministrado nas dependências da PREFEITURA, com exceção da **solução de monitoramento de performance de aplicações** e **solução de monitoramento de experiência digital** que poderão ser ministrados remotamente à equipe da PREFEITURA.

10.3. As despesas decorrentes do serviço de Treinamento serão de exclusiva responsabilidade da CONTRATADA, dentre eles (mas não se limitando a estes), instrutores, confecção do material didático, despesas de transporte, estadia e alimentação do instrutor, etc;

10.4. O pagamento pelos serviços de capacitação ficará condicionado à emissão, pela PREFEITURA, do "Termo de Aceite de Serviço", emitido por turma.

### 10.4.1. SOLUÇÃO NGFW COM IPS, CONTROLE DE APLICAÇÕES, VPN E AUTENTICAÇÃO MULTIFATOR

10.4.1.1. O instrutor deverá ser certificado na solução ofertada.

10.4.1.2. O treinamento "Hands-on" deverá ter a carga horária mínima de 40 (quarenta) horas.

10.4.1.3. O Treinamento poderá ser ministrado para até quatro colaboradores indicados pela PREFEITURA.

10.4.1.4. A CONTRATADA também deverá fornecer, além do treinamento não-oficial, o Treinamento Oficial de FABRICANTE com duração de pelo menos 40 (quarenta) horas para até três colaboradores para o NGFirewall e VPN, indicados pela PREFEITURA, nas instalações de um centro autorizado pelo fabricante, na cidade de São Paulo, sujeito a disponibilidade de turma.

10.4.1.5. Ao final do treinamento deverá ser emitido certificado de conclusão para cada aluno que concluir o curso.

### 10.4.2. SOLUÇÃO DE POLÍTICA DE SEGURANÇA E AUTENTICAÇÃO À REDE (NAC)

10.4.2.1. O instrutor deverá ser certificado na solução ofertada.

10.4.2.2. O treinamento "Hands-on" deverá ter a carga horária mínima de 40 (quarenta) horas.

10.4.2.3. O Treinamento poderá ser ministrado para até quatro colaboradores indicados pela PREFEITURA.

10.4.2.4. A CONTRATADA também deverá fornecer, além do treinamento não-oficial, o Treinamento Oficial de FABRICANTE com duração de pelo menos 40 (quarenta) horas para até três colaboradores para a Solução de NAC, indicados pela PREFEITURA, nas instalações de um centro autorizado pelo fabricante, na cidade de São Paulo, sujeito a disponibilidade de turma.

10.4.2.5. Ao final do treinamento deverá ser emitido certificado de conclusão para cada aluno que concluir o curso.

### 10.4.3. SOLUÇÃO DE PROTEÇÃO DE DNS RECURSIVO

10.4.3.1. O instrutor deverá ser certificado na solução ofertada.

10.4.3.2. O Treinamento Oficial do FABRICANTE com duração de pelo menos 24 (vinte e quatro) horas.

10.4.3.3. O Treinamento poderá ser ministrado online ou nas instalações da CONTRATADA para até quatro colaboradores indicados pela PREFEITURA.

10.4.3.4. Ao final do treinamento deverá ser emitido certificado de conclusão para cada aluno que concluir o curso.

10.4.4. **SOLUÇÃO DE MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E MONITORAMENTO DE EXPERIÊNCIA DIGITAL**

10.4.4.1. O Treinamento não-oficial (ou repasse de conhecimento Hands-on) deverá ser ministrado remotamente a equipe da PREFEITURA sobre a Solução de Performance de Aplicação e Experiência Digital, com no mínimo 24 (vinte e quatro) horas de duração;

10.4.4.2. O(s) instrutor(es) deverá ser certificados na soluções ofertadas;

10.4.4.3. O Treinamento poderá ser ministrado para até quatro colaboradores indicados pela PREFEITURA.

10.4.4.4. A CONTRATADA também deverá fornecer, além do treinamento não-oficial, o Treinamento Oficial de FABRICANTE com duração de pelo menos 40 horas para 08 (oito) alunos, sendo realizado em uma única turma;

10.4.4.5. É obrigatório um mínimo de 40 (quarenta) horas úteis de carga horária para cada turma;

10.4.4.6. O Treinamento poderá ser ministrado online ou nas instalações da CONTRATADA para até quatro colaboradores indicados pela PREFEITURA.

10.4.4.7. Ao final do treinamento deverá ser emitido certificado de conclusão para cada aluno que concluir o curso.

## ANEXO I.b. - REQUISITOS DE ATENDIMENTO DO SOC

| REQUISITOS DE ATENDIMENTO | | | | |
|---|---|---|---|---|
| **ITEM** | **DESCRIÇÃO** | **ATENDE** | **NÃO ATENDE** | **EVIDÊNCIA** |
| 1 | Centro de Operações de Segurança (Security Operation Center - SOC), incluindo minimamente dois ambientes na CONTRATADA, redundantes entre si e distantes, com pelo menos, 40 km de distância geodésica um do outro. | | | |
| 2 | 2 (dois) Centros de Operações de Segurança (SOC), já devem estar em pleno funcionamento na data da diligência, redundantes, de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados. | | | |
| 3 | Pelo menos 01 (um) dos Centros de Operações de Segurança (SOCs) deverá estar a no máximo 40 km de distância da Prefeitura, para permitir a participação efetiva da CONTRATADA em “War Room” ou salas de crise para momentos de crise. | | | |
| 4 | Sistema de registro individual e controle de visitante | | | |
| 5 | Circuito interno de gravação de imagem | | | |
| 6 | Funcionamento em regime 24x7x365 | | | |
| 7 | SOCs conectados aos Data Centers que hospedam os sistemas de suporte técnico, monitoramento, administração e gerenciamento através de múltiplas conexões de rede local ou WAN, de forma que a falha de uma conexão isoladamente não afete o acesso aos mesmos | | | |
| 8 | Possuir estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento que permita que todos os profissionais visualizem eventos relevantes simultaneamente. | | | |
| 9 | Possuir UPS que suporte todos os equipamentos essenciais ao funcionamento, por, pelo menos, 30 minutos. | | | |
| 10 | Possuir sistemas redundantes para armazenamento de dados e alimentação de energia. | | | |
| 11 | Segregação lógica da infraestrutura e sistemas utilizados na prestação do serviço | | | |

| | | | | |
|---|---|---|---|---|
| 12 | Estar configurados de forma que a falha de nenhum dos equipamentos isoladamente interrompa o funcionamento dos sistemas | | | |
| 13 | Possuir dispositivos redundantes para fornecer energia elétrica e controle de temperatura. Cada um destes dispositivos deve ter capacidade para manter a operação isoladamente em caso de manutenção planejada ou falha. | | | |
| 14 | Possuir caminhos de distribuição de energia elétrica, fluidos e gases para refrigeração e conexões de rede local redundantes de modo que um caminho permaneça ativo e o outro possa ser utilizado como alternativa em caso de manutenção planejada ou falha. Os sistemas de distribuição que devem ser considerados nessa especificação são: Cabine para recebimento de energia externa; Cabeamento de transmissão de energia; Quadros de distribuição; Dutos de água gelada (quando utilizados); Cabos para conexões de rede | | | |
| 15 | Possuir múltiplas entradas independentes para fornecimento de energia elétrica. Cada entrada para fornecimento de energia elétrica deve ser capaz de isoladamente suportar a operação do data center | | | |
| 16 | Possuir múltiplas conexões independentes para acesso à Internet. Cada conexão para acesso à Internet deve ser capaz de suportar isoladamente a operação do data center. | | | |

**ANEXO I.c. - TERMO DE CONFIDENCIALIDADE E PROTEÇÃO DE DADOS**

CONTRATO Nº _____ /__

O presente TERMO DE CONFIDENCIALIDADE E PROTEÇÃO DE DADOS rege a divulgação de informações entre a CONTRATADA,, estabelecida(o) a , Município, inscrita(o) no Cadastro Nacional de Pessoas Jurídicas – CNPJ/MF sob nº, neste ato representada(o) por ao final assinado, e a PREFEITURA DE SANTANA DE PARNAÍBA, Avenida Marechal Mascarenhas de Moraes, 1283 – Sítio do Morro – Santana de Parnaíba/SP - CEP: 06517-520, inscrito no CNPJ/MF sob n º 46.522.983/0001-27, doravante denominada PREFEITURA, neste ato, por seu representante legal ao final assinalado, o qual, a partir do reconhecimento deste ato, dá conhecimento e estabelece as regras de confidencialidade e de proteção de dados a serem observadas pelas partes:

1. A CONTRATADA DECLARA e compromete-se:

a. A cumprir rigorosamente as normas regulamentares sobre a utilização dos meios e infraestrutura, bem como as diretrizes estipuladas pela PREFEITURA DE SANTANA DE PARNAÍBA, mantendo a confidencialidade em relação a toda a documentação e à coleta de dados pessoais (sensíveis ou não) indispensáveis à prestação do serviço, se houver. Os dados assim coletados, bem como os dados pessoais sensíveis, somente poderão ser utilizados na execução dos serviços especificados neste contrato, conforme disposto, respectivamente, nos artigos 8º, § 1º e art. 11, incisos I e II, da LGPD, em hipótese alguma poderão ser compartilhados ou utilizados para outros fins. Não haverá a possibilidade de tratamento posterior de forma incompatível com essas finalidades (inciso I do art. 6º da LGPD), bem como serão consideradas nulas as autorizações genéricas (§ 4º do art. 8º da Lei nº 13.709, 2018). A CONTRATADA, nos termos do art. 7º, § 5º, da LGPD, obriga-se a obter o consentimento do(s) respectivo(s) titular(es), sempre que a disponibilização dos dados a PREFEITURA assim o requerer. Em se tratando de dados disponibilizados pela PREFEITURA à CONTRATADA, a PREFEITURA obterá o consentimento do(s) respectivo(s) titular(es), sempre que a lei assim o requerer, após solicitação da CONTRATADA;

b. A armazenar os dados obtidos em razão desse contrato em um banco de dados seguro, mantido em território nacional, com transparente identificação do perfil dos credenciados, garantindo-se a rastreabilidade de cada transação e a franca apuração, a qualquer tempo, de desvios e falhas, vedado seu compartilhamento com terceiros;

c. Não divulgar as informações obtidas nas atividades exercidas junto a PREFEITURA DE SANTANA DE PARNAÍBA, exceto quando expressamente autorizada pela PREFEITURA DE SANTANA DE PARNAÍBA;

d. Não permitir que qualquer pessoa manuseie qualquer documento físico ou eletrônico que componha ou tenha resultado de atividades da PREFEITURA, exceto se devidamente autorizada;

e. Não explorar, em benefício próprio ou de terceiros, informações e documentos adquiridos através da participação em atividades da PREFEITURA;

2. DECLARA AINDA CIÊNCIA de que:

a. Qualquer divulgação oral ou eletrônica, que acompanhe a informação escrita, também será considerada Informação Confidencial. Se a informação for divulgada oral ou eletronicamente sem documentação escrita acompanhando, também será considerada Informação Confidencial, salvo manifestação expressa em contrário da Parte Divulgadora quando da divulgação;

b. Dará conhecimento formal aos seus empregados, representantes, prepostos, consultores ou qualquer terceiro que tenha conhecimento da presente contratação, das obrigações e condições acordadas neste item, bem como da Política de Privacidade da PREFEITURA, cujos princípios deverão ser aplicados à coleta e tratamento dos dados pessoais (sensíveis ou não) de que trata a presente cláusula, responsabilizando-se por toda e qualquer operação realizada em desacordo com a Lei nº 13.709/2018 e/ou outros normativos que venham a entrar em vigor sobre proteção de dados;

c. As partes se comprometem a proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, inerentes ao tratamento de dados pessoais, inclusive nos meios digitais. Aa PREFEITURA, por sua vez, é reservada a prerrogativa de monitorar e auditar quaisquer atividades que envolvam dados ou informações cuja perda ou vazamento possa trazer graves implicações a PREFEITURA ou consequências administrativas, civis ou criminais aos responsáveis por sua violação, notadamente por meio do representante especialmente designado, a que se refere o art. 67 da Lei de Licitações e Contratos Administrativos;

d. Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a CONTRATADA providenciará seu descarte de forma segura, comunicando a PREFEITURA;

e. A CONTRATADA deverá comunicar a PREFEITURA, no prazo de 24 (vinte e quatro) horas da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais sensíveis ou não, a fim de viabilizar a adoção das providências devidas;

f. As partes se comprometem a adotar as melhores práticas de Proteção de Dados, conforme Lei nº 13.709/2018 e/ou outros normativos que venham a entrar em vigor sobre proteção de dados;

g. a PREFEITURA deverá, considerando os meios tecnológicos disponíveis e adequados às suas atividades, a natureza dos dados armazenados e os riscos a que estão expostos, adotar medidas físicas e lógicas, de caráter técnico e organizacional, a fim de prover a confidencialidade e a segurança de seus dados, evitar sua alteração, perda, subtração ou acesso não autorizado, bem como a violação da privacidade dos sujeitos titulares dos dados;

h. O descumprimento das obrigações relacionadas à confidencialidade e à segurança de dados, de informações e sistemas, mediante ações ou omissões, intencionais ou acidentais, que impliquem perda, destruição, inserção, cópia, acesso ou alterações indevidas, independentemente do meio no qual estejam armazenados, em que trafeguem ou do ambiente em que estejam sendo processados, determinará a responsabilização, na forma da lei, de seus dirigentes e funcionários envolvidos, sem prejuízo das sanções estabelecidas, no presente contrato. Desse modo, as partes responderão administrativa e judicialmente, e, em solidariedade com os agentes de tratamento, estes conceituados nos incisos VI, VII e VIII do art. 5ª da Lei nº 13.709/2018, em caso de causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD, conforme previsto em seu art. 42, § 1º, inciso I;

i. O presente Acordo somente poderá ser alterado mediante consentimento mútuo e Aditamento por escrito, assinado por ambas as partes. As obrigações de confidencialidade contidas no presente TERMO DE CONFIDENCIALIDADE E PROTEÇÃO DE DADOS se perpetuarão por tempo indeterminado, independente do término da vigência do CONTRATO.

_____

PREFEITURA DE SANTANA DE PARNAÍBA

_____

CONTRATADA

## ANEXO I.d – VALIDAÇÃO SOLUÇÕES (PoC) ANEXO I.a

| REQUISITOS DE ATENDIMENTO | | | | |
|---|---|---|---|---|
| **ITEM** | **DESCRIÇÃO** | **ATENDE** | **NÃO ATENDE** | **EVIDÊNCIA** |
| **1** | Solução NGFW com IPS, controle de aplicações, VPN e autenticação multifator | | | |
| **2** | Solução de política de segurança e autenticação à rede (NAC) | | | |
| **3** | Solução de proteção de DNS recursivo | | | |
| **4** | Solução de monitoramento de performance de aplicações | | | |
| **5** | Solução de Monitoramento de experiência digital | | | |

# ANEXO II
## *Justificativas Complementares*

**1. Justificativa pela não exclusividade de itens para ME/EPP e pela não separação dos itens para cotas reservadas para ME/EPP**

1.1. O objeto será agrupado em **lote único** pelo fato de que o fornecedor deverá efetuar configurações e integrações entre todos os produtos. O agrupamento de itens também permite o alcance de maior eficiência não só no âmbito da funcionalidade da contratação, como também naquele relacionado à prevenção de contratações conflituosas e, por conseguinte, redução de conflitos entre fornecedores distintos. O modelo de contratação pretendido permite a preservação do funcionamento integrado, não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, o suporte técnico e o treinamento serão executados por um único fornecedor por grupo. Dessa forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução.

1.2. Considerando que o valor total do presente certame supera o de 80 mil reais, valor previsto para realização de licitações exclusivas;

1.3. Considerando que o objeto não é divisível, pois os serviços não podem ser desmembrados;

1.4. Considerando que no entendimento do TCE-SP (Tribunal Pleno do TCE/SP: TC-025129.989.20-8, TC-025128.989.20-9 e TC-025130.989.20-5), no sentido de que as prestações de serviço não são fracionáveis, por consequente, não sendo possível seu desmembramento (reserva de cota);

1.5. Considerando ainda que a Ampla Concorrência não impede a participação de empresas enquadradas como ME/EPP/MEI/COOP;

1.6. Para fins de participação nesta licitação, justificada a impossibilidade e inviabilidade de atendimento dos artigos 47 a 48 da LC 123/06 e alterações, e tendo em vista a iminente desvantagem e prejuízo para a contratação, o certame será aberto para competição de todas as empresas que atenderem às exigências deste edital, e, não serão reservadas cotas, exclusividade ou subcontratação para ME/EPP/MEI/COOP, à exceção da regularidade fiscal e trabalhista postergada e da preferência em caso de empate ficto que se aplicam integralmente.

**2. Da Fiscalização:**

**1.1. Fiscalização Técnica**

1.1.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

1.1.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

1.1.3. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

1.1.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

1.1.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

**1.2. Fiscalização Administrativa**

1.2.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

1.2.2. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

**1.3. Gestor do Contrato**

1.3.1. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais. (Decreto nº 11.246, de 2022, art. 21, IV).

1.3.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

1.3.3. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

1.3.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

1.3.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

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

3.

# ANEXO III

## ***Planilha de Itens e Valores Estimados***

| LOTE - SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES COMPLEMENTARES DE SEGURANÇA DE REDES E APLICAÇÕES | | | | | | |
|---|---|---|---|---|---|---|
| **Item** | **Código Interno** | **Qtde** | **Especificação** | **Un. Med.** | **Média Unit.** | **Média dos Orçamentos** |
| **1.1** | 194288 | 48 | SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES | Sv | R$ 185.972,2900 | R$ 8.926.669,92 |
| **1.2** | 194289 | 48 | SERVIÇO DE RESPOSTA A INCIDENTES CIBERNÉTICOS | Sv | R$ 20.458,0033 | R$ 981.984,16 |
| **1.3** | 194290 | 15 | SERVIÇOS TÉCNICOS CONTINUADOS DE SOLUÇÕES CISCO | Sv | R$ 24.294,5800 | R$ 364.418,70 |
| **1.4** | 194291 | 15 | SERVIÇOS TÉCNICOS DE WIFI | Sv | R$ 16.960,4667 | R$ 254.407,00 |
| **1.5** | 194292 | 1 | SERVIÇO DE TREINAMENTO DAS SOLUÇÕES (NGFW, VPN, MFA, NAC, DNS, MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E EXPERIÊNCIA DIGITAL) | Sv | R$ 333.696,3767 | R$ 333.696,38 |
| **1.6** | 194293 | 1 | SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DAS SOLUÇÕES NGFW, VPN, MFA, NAC, DNS, MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E EXPERIÊNCIA DIGITAL | Sv | R$ 771.907,6433 | R$ 771.907,64 |
| **1.7** | 194294 | 400 | HORAS DE CONSULTORIA PARA SOLUÇÃO DE MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES | Sv | R$ 492,0000 | R$ 196.800,00 |
| **TOTAL LOTE / GLOBAL** | | | | | | **R$ 11.829.883,80** |

**ANEXO IV**

***Relação de Documentos de Habilitação***

**DA HABILITAÇÃO**

**Toda a documentação abaixo deverá ser encaminhada para fins de HABILITAÇÃO em conformidade com o edital.**

**1. HABILITAÇÃO JURÍDICA**

**1.1** Instrumentos contratuais, conforme cada caso:

**a)** Prova de registro empresarial na junta comercial, no caso de empresa individual;

**b)** Instrumento constitutivo, estatuto ou contrato social em vigor devidamente registrado na Junta Comercial, em se tratando de sociedade empresarial e no caso de sociedades por ações acompanhadas de documentos de eleição de seus administradores.

**c)** Instrumento constitutivo devidamente registrado no Cartório de Registro Civil de Pessoas Jurídicas tratando-se de sociedades não empresárias, acompanhado de prova da diretoria em exercício;

**d)** Decreto de autorização e ato de registro ou autorização para funcionamento expedido pelo órgão competente, tratando-se de empresa ou sociedade estrangeira em funcionamento no país, quando a atividade assim o exigir;

**e)** No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

**1.1.1** Os instrumentos deverão ser apresentados na última alteração consolidada ou através de cópia de todas as alterações de forma a comprovar o histórico da empresa.

**1.1.2** Caso o tipo societário elencado acima for impedido por lei de atuar no ramo/objeto do certame, favor desconsiderar, já que os itens são padrão e utilizados em todos editais.

**1.2** Em se tratando de **consórcios,** conforme determina o art. 15, da Lei Federal no 14.133/21, deverão ser observadas as seguintes regras:

**I -** comprovação de compromisso público ou particular de constituição de consórcio, subscrito pelos consorciados;

**II -** indicação da empresa líder do consórcio, que será responsável por sua representação perante a Administração;

**III -** admissão, para efeito de habilitação técnica, do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, do somatório dos valores de cada consorciado;

**IV -** impedimento de a empresa consorciada participar, na mesma licitação, de mais de um consórcio ou de forma isolada;

**V -** responsabilidade solidária dos integrantes pelos atos praticados em consórcio, tanto na fase de licitação quanto na de execução do contrato.

**1.2.1** A Licitante deverá apresentar **Declaração de obrigação** do licitante, que caso seja vencedor, promoverá antes da celebração do contrato, na forma do art. 15, § 3º da Lei Federal 14.133/21, a constituição e o registro do consórcio;

**1.2.2** A apresentação dos documentos relativos à regularidade jurídica e fiscal e trabalhista deverá ser atendida por cada uma das empresas consorciadas;

**1.2.3** As empresas reunidas em consórcio deixam de gozar dos benefícios admitidos neste edital no que se refere ao Direito de Preferência elencados na Lei nº 123/06, se todas não estiverem enquadradas nesta condição ou se houver vedação do benefício devido ao valor ou ao tipo do objeto a ser contratado;

**1.2.4** A empresa líder do consórcio será responsável perante a Concedente pelo compromisso do contrato, sem prejuízo da responsabilidade solidária das demais consorciadas.

**2. REGULARIDADE FISCAL e TRABALHISTA:**

**2.1** Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ) ou no Cadastro de Pessoas Físicas (CPF) (quando permitido), conforme o caso;

**2.2** Prova de inscrição no Cadastro de Contribuintes Estadual e/ou Municipal, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

**2.3** Prova de regularidade para com a:

**a) Fazenda Federal** - Certidão Conjunta de Débitos relativos a Tributos Federais e à Dívida Ativa da União e prova de regularidade relativa à Seguridade Social (INSS), expedida pela Receita Federal e Procuradoria Geral da Fazenda Nacional (https://solucoes.receita.fazenda.gov.br/Servicos/certidaointernet/PJ/Emitir); e

**b) Fazenda Municipal** – Negativa de Tributos Mobiliários do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

a. *Caso o fornecedor seja considerado isento dos tributos Estadual e/ou Municipal relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei*.

**2.4** Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço (**FGTS**), por meio de Certificado de Regularidade Fiscal (CRF), expedido pela Caixa Econômica Federal (https://consulta-crf.caixa.gov.br/consultacrf/pages/consultaEmpregador.jsf), ou documento equivalente, com prazo de validade em vigor na data marcada para abertura da sessão e processamento do pregão;

**2.5** Prova de inexistência de débitos inadimplidos perante a **Justiça do Trabalho**, por meio de Certidão Negativa de Débitos Trabalhistas (**CNDT**), expedida pelo Tribunal Superior do Trabalho (www.tst.jus.br/certidao) conforme Lei nº 12.440/2011 e Resolução Administrativa TST nº 1470/2011;

**2.6** A Comprovação de regularidade fiscal e/ou trabalhista das microempresas e empresas de pequeno porte será exigida, como definido em edital a na legislação aplicável.

**As provas de regularidade deverão ser feitas por Certidão Negativa ou Positiva com Efeitos de Negativa**.

**3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:**

**3.1** Apresentar **Certidão negativa de** falência expedida pelo distribuidor da sede do fornecedor ou do domicílio do empresário individual a menos de 90 (noventa) dias da data prevista para abertura da sessão (ou conforme validade do documento se constar data), observando ainda o que segue:

**3.1.1** Se a licitante for **sociedade não empresária (sociedade simples, etc.)**, ou pessoa física (quando permitido) a certidão mencionada no item 3.1 deverá ser substituída por certidão cujo conteúdo **demonstre a ausência de insolvência civil**, expedida pelo distribuidor do domicílio ou sede do licitante;

**3.2** As empresas participantes deverão comprovar possuir **Capital Social** mínimo de 10% (dez por cento) sobre a somatória **da estimativa** dos ITENS/LOTES que ofertarem proposta ou sobre o valor total estimado desta licitação para os que participarem de todos os ITENS/LOTES e quando se tratar de licitação global (observado neste caso a exigência do percentual referente ao período equivalente a 12 meses).

**3.3** As empresas que não atenderem a qualificação econômico-financeira através do Capital Social poderão comprovar qualificação financeira através do: **Patrimônio Líquido** mínimo de 10% (dez por cento) sobre a somatória da estimativa dos ITENS/LOTES em que participar ou sobre o valor total estimado desta licitação (observado neste caso a exigência do percentual referente ao período equivalente à 12 meses) para os que participarem de todos os ITENS/LOTES (e licitação global), devendo, para essa finalidade, extraí-los dos números apresentados no **Balanço Patrimonial.**

**3.3.1** Para que produza os efeitos esperados deve ser apresentado o **Balanço Patrimonial do ÚLTIMO EXERCÍCIO exigível (e suas Demonstrações Contábeis)** nas formas da lei, atendendo às seguintes exigências mínimas:

**a)** Para as Pessoas Jurídicas regidas pela Lei n° 6.404/76 (**Sociedades Anônimas** – S/A): **apresentar Balanço nos termos da alínea "e" deste item**, devendo ainda ser apresentada a publicação do recibo do SPED ou do resumo em jornais de grande circulação e/ou em sítios oficiais, observando qualquer outra obrigação constante na legislação aplicável, conforme cada caso;

**b)** Para as **Pessoas Jurídicas em geral**: apresentar cópia do Balanço e Demonstrações de Resultado do Exercício contábil – DRE, juntamente com os Termos de Abertura e Encerramento (todos extraídos do Livro Diário físico ou de Livro Digital – desde que admitido na junta comercial de seu Estado e que atenda às formalidades inerentes ao arquivamento dos livros contábeis nas formas da legislação aplicável), devidamente **Registrados** na Junta Comercial ou no Cartório de Registro (no caso das Sociedades Simples) da sede ou domicílio da licitante;

**c)** Para as **Pessoas Jurídicas criadas no exercício em curso** ou com criação em período anterior ao limite exigido para registro legal do Balanço completo: deverão apresentar cópia do Balanço de Abertura, devidamente **Registrado** na Junta Comercial ou no Cartório de Registro, conforme explanado na alínea "b" deste item;

**d)** Para as Pessoas Jurídicas sujeitas ao regime estabelecido na **Lei Complementar nº 123/06** (Microempreendedor Individual, Microempresa, Empresa de Pequeno Porte e Cooperativa de Consumo): devem atender às mesmas **regras dispostas nas alíneas "b", "c" ou "e"**, conforme cada caso, não sendo aceitos "balanços ou contabilidade simplificados";

**e)** Para as Pessoas Jurídicas **optantes ou obrigadas** à Escrituração Contábil Digital (ECD), parte integrante do **SPED** (Sistema Público de Escrituração Digital), nos termos dos Decretos nº 6.022 de 22/01/2007, nº 8.683 de 25/08/2016, e nº 9.555 de 06/11/2018; da Instrução Normativa RFB Nº 2003 de 18/01/2021, alterações destas e demais legislações aplicáveis: devem apresentar o Balanço e a Demonstração de Resultado do Exercício – DRE, com os respectivos Termos de Abertura e Encerramento e com o **Recibo de Entrega** emitido pelo SPED com o mesmo código de autenticação do rodapé dos demais documentos apresentados para que seja possível verificar a autenticidade das informações apresentadas.

**3.4** As empresas que não atenderem ao Capital Social ou Patrimônio Líquido nos termos dos subitens **3.2** e **3.3 e seguintes**, devem apresentar os **cálculos dos Índices de Liquidez juntamente com os Balanços Patrimoniais DOS DOIS ÚLTIMOS EXERCÍCIOS exigíveis na forma da Lei (apresentados nos termos das alíneas do subitem 3.3.1)** a fim de comprovarem sua boa situação financeira ao atender ou superar os índices a seguir expostos **EM AMBOS OS EXERCÍCIOS,** sob pena de inabilitação:

$$ILC = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}} \geq 1{,}00$$

$$ILG = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{} \geq 1{,}00$$

$$IS = \frac{\text{ATIVO TOTAL}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}} \geq 1{,}00$$

Onde " ≥ " maior ou igual.

Sendo:

**ILC = índice de liquidez corrente**

**ILG = índice de liquidez geral**

**IS = índice de solvência**

**3.5** As empresas que comprovarem a qualificação econômico-financeira da forma tratada no item **3.2** estão **DESOBRIGADAS** de apresentar Balanço Patrimonial e/ou o Cálculo dos Índices, **porém, a apresentação do Balanço e dos Índices de Liquidez é indicação bastante de que as empresas desejam se utilizar destes para comprovarem a qualificação exigida nos itens acima;**

**3.5.1** A apresentação do Balanço e dos Índices implica **na obrigação por parte da Administração** de análise e consideração da legalidade quanto à forma de apresentação acima tratadas, sendo ignorada a opção disposta no item 3.2.

**4. DOCUMENTAÇÃO TÉCNICA E/OU COMPLEMENTAR:**

**4.1** Assinalar as declarações obrigatórias como condição de participação, exigidas no cadastramento da Proposta Comercial no sistema.

**4.2** Conforme previsto no item 9.6 a 9.12 e 9.15 do ANEXO – I.

# ANEXO V
## *Modelo de Proposta Comercial*
## *PREGÃO ELETRÔNICO Nº XXX/2024*

***INFORMAR OS DADOS CADASTRAIS DA EMPRESA EM PAPEL TIMBRADO***
*(NA PROPOSTA FÍSICA)*

**Obs:** Adverte-se que a simples apresentação da Proposta Eletrônica será considerada como indicação bastante de que inexistem fatos que impeçam a participação da licitante neste certame, ou de que a mesma não foi declarada inidônea para licitar ou contratar com a Administração Pública, e que atende a todos os itens descritos e exigidos nos Anexos I, I.a, I.b, I.c e III.

| LOTE - SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES COMPLEMENTARES DE SEGURANÇA DE REDES E APLICAÇÕES | | | | | |
|---|---|---|---|---|---|
| **Item** | **Qtde** | **Especificação** | **Un. Medida** | **Valor Unit.** | **Valor Total** |
| **1.1** | 48 | SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES | Sv | R$ | R$ |
| **1.2** | 48 | SERVIÇO DE RESPOSTA A INCIDENTES CIBERNÉTICOS | Sv | R$ | R$ |
| **1.3** | 15 | SERVIÇOS TÉCNICOS CONTINUADOS DE SOLUÇÕES CISCO | Sv | R$ | R$ |
| **1.4** | 15 | SERVIÇOS TÉCNICOS DE WIFI | Sv | R$ | R$ |
| **1.5** | 1 | SERVIÇO DE TREINAMENTO DAS SOLUÇÕES (NGFW, VPN, MFA, NAC, DNS, MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E EXPERIÊNCIA DIGITAL) | Sv | R$ | R$ |
| **1.6** | 1 | SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DAS SOLUÇÕES NGFW, VPN, MFA, NAC, DNS, MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES E EXPERIÊNCIA DIGITAL | Sv | R$ | R$ |
| **1.7** | 400 | HORAS DE CONSULTORIA PARA SOLUÇÃO DE MONITORAMENTO DE PERFORMANCE DE APLICAÇÕES | Sv | R$ | R$ |
| | | | | **Total Geral:** | |

**Valor Total por extenso:** _____

**a)** Da execução/fornecimento: conforme disposto no Anexo I – Termo de Referência.

**b)** Validade da proposta (mínimo 60 dias): _____.

**c)** Prazo de pagamento: de até 30 (trinta) dias, contados da data do aceite da nota fiscal pela secretaria requisitante.

**d)** Da vigência: 60 (sessenta) meses, contados a partir da data de recebimento da ORDEM DE SERVIÇOS pela Contratada, emitida pela Secretaria Municipal de Administração;

1) Deve ser apresentada, juntamente com a proposta comercial a tabela com a relação total dos partnumbers, indicando os componentes em uso e capacidades dos mesmos, com

breve explicação/descrição dos componentes para facilitar a interpretação pela PREFEITURA de acordo com o **item 9.14.1 do Termo de Rereferência**, conforme o exemplo abaixo:

| ITEM COMO SERVIÇO | RELAÇÃO DE PARTNUMBER (SKU) | DESCRIÇÃO | OBSERVAÇÃO / DETALHAMENTO |
|---|---|---|---|
| Solução NGFW com IPS, controle de aplicações, VPN e autenticação multifator em alta disponibilidade | IIIIIIIIIIIIII | Licença IIIIIIIIIIIIII | SOLUÇÃO COMPOSTA POR ..... |
| | JJJJJJJJJJJJ | SUPORTE 24x7, COM DURAÇÃO DE _____ ANOS | JJJJJJJJJJJJ, com duração de ____ para ____ |
| Solução de política de segurança e autenticação à rede (NAC) | XXXXXXX | Licença XXXXXX | SOLUÇÃO COMPOSTA POR ___ |
| | LLLLLLLLLL | SUPORTE 24x7, COM DURAÇÃO DE ___ ANOS | LLLLLLLLLL, com duração de ___ para ___ |
| Solução de proteção de DNS recursivo | WWWW | Licença WWWW | WWWWW, com duração de ___ para ___ |
| | XXXXXXX | Suporte XXXXXXX | XXXXXXX, com duração de ___ para ___ |
| | YYYYYYY | Licença YYYYYYY | YYYYYYY, com duração de ___ para ___ |
| | ZZZZZZZZ | SUPORTE 24x7, COM DURAÇÃO DE ZZ ANOS | ZZZZZZZZ, com duração de ___ para ___ |
| Solução de monitoramento de performance de aplicações | AAAAAAAA | Licença de AAAAAA MODELO: AAAAAA | SOLUÇÃO COMPOSTA POR ___ |
| | BBBBBBBBB | Suporte BBBBBBB | BBBBBBB, com duração de ___ |
| | CCCCCCCCC | Licença CCCCCC | CCCCC ___ |
| | DDDDDDD | SUPORTE DDDDD | DDDD ___ |
| | EEEEEEEEE | SUPORTE 24x7, COM DURAÇÃO DE EE ANOS | ATENDIMENTO ONSITE, COM REPOSIÇÃO DE PEÇAS EM ATÉ ___ |
| Solução de Monitoramento de experiência digital | FFFFFFFFFF | Licença de FFFFFFFFFF MODELO: FFFFFFFFFF | SOLUÇÃO COMPOSTA POR ___ |
| | GGGGGGG | Suporte GGGGGGG | GGGGGGG, com duração de ___ |

1) Não serão aceitas descrições que não estejam acompanhadas individualmente por item/subitem de documento comprobatório com os itens da tabela.
2) A CONTRATADA deverá enviar a comprovação técnica das especificações e certificações dos produtos ofertados por meio de documentos públicos, tais como certificados, catálogos, manuais ou sites oficiais dos fabricantes dos produtos ofertados.
    a. Entenda-se como documentos públicos quaisquer documentos impressos ou eletrônicos disponíveis para o público em geral até a data de publicação do presente edital.
3) Todas as comprovações técnicas e/ou certificações devem ser apresentadas obrigatoriamente na proposta comercial, assim como o **Plano e Cronograma de Implantação das Soluções descrita no item 9.14.2.**

**Declaro, sob as penas da lei, que os produtos ofertados atendem todas as especificações exigidas por esta licitação, bem como dos itens de detalhamento do Anexo I - Termo de Referência e Anexo III – Planilha de Itens e Valores Estimados.**
**Declaro ainda, que os preços acima indicados contemplam todos os custos operacionais da atividade e os tributos eventualmente incidentes, bem como as despesas diretas e indiretas, inclusive o transporte e mão de obra necessários à entrega, fornecimento e instalação deste objeto.**

Nome do representante legal da empresa que assinará e será responsável pelo instrumento: _____.
CPF: _____ RG: _____.
Telefone: (____)_____ Fax: (____)_____.
e-mail pessoal: _____.
e-mail profissional: _____.
Data de nascimento do responsável: _____.

**Dados bancários:**
Nome do Banco: _____ Nº do Banco: _____
Agência:_____ c/c: _____

Assinatura: _____
Nome do responsável: _____
R.G.: _____
C.P.F.: _____

(assinatura do representante)

**Cidade, data e dados do representante**

**ANEXO VI**

***Minuta de Termo de Contrato***

**PREFEITURA MUNICIPAL DE SANTANA DE PARNAÍBA**

***PROCESSO ADMINISTRATIVO Nº 240319028916000/2024***

***CONTRATO N.º. ...../2024 / QUE FAZEM ENTRE SI O MUNICÍPIO DE SANTANA DE PARNAÍBA E A EMPRESA .....***

Aos ..... (.....) dias do mês de ..... 2024 (dois mil e vinte e quatro) nesta cidade de Santana de Parnaíba - SP, compareceram as partes entre si justas e contratadas, a saber: de um lado o **MUNICÍPIO DE SANTANA DE PARNAÍBA**, pessoa jurídica de direito público interno, com sede à Avenida Marechal Mascarenhas de Moraes, 1283 - Sítio do Morro - Santana de Parnaíba - SP, inscrita no CNPJ sob n.º 46.522.983/0001-27, neste ato representada pelo seu Prefeito Municipal **ANTONIO MARCOS BATISTA PEREIRA**, a seguir denominada simplesmente **"CONTRATANTE"**, e de outro lado, a Empresa ....., estabelecida na cidade de ....., à ....., n.º ....., inscrita no CNPJ sob n.º ....., neste ato representada pelo seu diretor....., doravante denominada simplesmente **"CONTRATADA"**, tendo em vista o que consta no Processo nº 240319028916000/2024 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº XXX/2024, na presença de duas testemunhas ao final assinadas, ficou justo e contratado o seguinte, que mutuamente outorgam e aceitam, a saber:

**CLÁUSULA I – DO OBJETO**

**1**. Contratação de empresa especializada para fornecer SERVIÇOS GERENCIADOS COM FORNECIMENTO DE SOLUÇÕES COMPLEMENTARES DE SEGURANÇA DE REDES E APLICAÇÕES, por um período de 48 (quarenta e oito) meses, nas quantidades e especificações descritas no Termo de Referência.

**1.2** Objeto da Contratação

| Item | Qtde | Especificação | Marca / Fabricante | Un. Medida | Valor Unit. | Valor Total |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | **Total Geral:** | |

**1.3** Vinculam esta contratação, independentemente de transcrição:

**1.3.1** O Termo de Referência;

**1.3.2** O Edital da Licitação;

**1.3.3** A Proposta do contratado;

**1.3.4** Eventuais anexos dos documentos supracitados.

**CLÁUSULA II – DA VIGÊNCIA E PRORROGAÇÃO**

**2.1 Da vigência do contrato:** 48 (quarente e oito) meses, contados a partir da data de recebimento da ORDEM DE SERVIÇOS pela Contratada, emitida pela Secretaria Municipal de Tecnologia da Informação - SMTI;

**2.2** O prazo deste Contrato pode ser prorrogado nos termos do art. 114 da Lei nº 14.133/23 e condições permitidas pela legislação vigente.

**CLÁUSULA III – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS**

**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 IV – SUBCONTRATAÇÃO**

**4.1** Não será admitida a subcontratação do objeto contratual.

**CLÁUSULA V – PREÇO**

**5.1** O valor total da contratação é de R$ ..... (.....)

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

**CLÁUSULA VI – PAGAMENTO**

**6.1** O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

**CLÁUSULA VII – REAJUSTE**

**7.1** Os preços serão reajustados nos termos permitidos pela legislação vigente considerando a data referência disposta nesta cláusula.

**7.1.1** Data referência do orçamento estimado**: 03/05/2024**;

**7.1.2** Especificamente para fins desta contração, o valor só poderá ser reajustado se comprovado motivo de força maior, decorrente de fato atípico que impeça a entrega no prazo. O reajuste deverá ser calculado proporcionalmente ao período e a parcela aplicável, pela variação do **Índice de Custos de Tecnologia da Informação – ICTI,** mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA.

**7.1.3.** Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

**7.1.4.** Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

**7.1.5.** O reajuste será realizado por apostilamento.

**CLÁUSULA VIII – OBRIGAÇÕES DA CONTRATANTE**

**8.1** São obrigações da **CONTRATANTE,** além das previstas no termo de referência:

**8.1.1** Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com o contrato e seus anexos;

**8.1.2** Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

**8.1.3** Notificar a Contratada, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

**8.1.4** Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela Contratada;

**8.1.5** Efetuar o pagamento à Contratada do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

**8.1.6** Aplicar à Contratada as sanções previstas na lei e neste Contrato;

**8.1.7** Cientificar o órgão de representação judicial da Prefeitura de Santana de Parnaíba para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

**8.1.8** 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;

**8.1.9** A Administração terá o prazo de 15 (quinze) dias corridos, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período;

**8.1.10** Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela contratada no prazo máximo de 30 (trinta) dias corridos;

**8.1.11** Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais;

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

**8.1.13** Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021

**CLÁUSULA IX – OBRIGAÇÕES DA CONTRATADA**

**9.1** A **CONTRATADA** deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando além das previstas no termo de referência, as obrigações a seguir dispostas:

**9.1.1** Entregar o objeto acompanhado do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada;

**9.1.2** responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

**9.1.3** comunicar a **CONTRATANTE**, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

**9.1.4** atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

**9.1.5** reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

**9.1.6** responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

**9.1.7** quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a **CONTRATADA** deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

**9.1.8** 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 e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

**9.1.9** Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual;

**9.1.10** 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;

**9.1.11** manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

**9.1.12** cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei n.º 14.133, de 2021);

**9.1.12.1** comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei n.º 14.133, de 2021);

**9.1.13** guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

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

**9.1.15** cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da **CONTRATANTE**;

**9.1.16** alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

**9.1.17** orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato;

**9.1.18** conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina;

**9.1.19** submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere;

**9.1.20** não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

**9.1.21** o fornecimento/serviço deverá atender a todas as normas de segurança, devendo quando for o caso, ser acompanhadas por técnico responsável na forma da Lei;

**9.2** em cumprimento às suas obrigações, cabe ainda à **CONTRATADA**, além das obrigações constantes das especificações e daquelas estabelecidas em lei, sobre licitações:

**9.2.1** responsabilizar-se integralmente pelos fornecimentos/serviços contratados, nos termos da legislação vigente;

**9.2.2** designar por escrito, no ato do recebimento da Ordem de Fornecimento/Serviço, preposto (supervisor) que tenha poderes para resolução de possíveis ocorrências durante a execução deste contrato;

**9.2.3** manter, durante toda a execução do contrato, a compatibilidade com as obrigações assumidas **(especialmente as exigências dos Anexos I – Termo de Referência e III – Planilha de Itens e Valores Estimados)**.

**CLÁUSULA X – DA GARANTIA CONTRATUAL**

**10.1** – **DA GARANTIA**

**10.1.1 Para a licitante vencedora** será exigida **garantia** para execução do contrato, nas modalidades previstas em Lei, **na importância de 3% (três por cento) do valor do contrato.** A garantia deverá ser apresentada na assinatura do ajuste.

**10.1.1.1** A garantia poderá ser prestada por uma das seguintes modalidades:

**a)** Caução em dinheiro ou títulos da dívida pública;

**b)** Seguro-garantia, na forma da legislação aplicável;

**c)** Fiança bancária **(emitida por instituição bancária autorizada pelo BACEN);**

**c.1)** A fiança bancária deverá conter:

**I.** Prazo de validade, que deverá corresponder ao período de vigência do contrato;

**II.** Expressa afirmação do fiador de que, como devedor solidário, fará o pagamento que for devido, independentemente de interpelação judicial, caso o afiançado não cumpra suas obrigações;

**III.** Renúncia expressa do fiador ao benefício de ordem e aos direitos previstos nos artigos 827 e 838 do Código Civil Brasileiro;

**IV.** Cláusula que assegure a atualização do valor afiançado.

**d)** Título de capitalização custeado por pagamento único, com resgate pelo valor total.

**CLÁUSULA XI – DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES**

**11.1** Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado 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 art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

**11.2** Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

**I. Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

**II. Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

**III. Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

**IV. Multa**:

**1.** Moratória de 0,10% (um décimo por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 15 (quinze) dias;

**2.** Moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o máximo de 10% (dez por cento), após o 15º e até o 30º dia de atraso. Após esse período, poderão ser aplicadas outras sanções, iniciando-se pela disposta no subitem 7 deste.

**2.1** Observa-se que o atraso superior a 15 quinze dias autoriza a Administração a promover a extinção do contrato, concomitante com a aplicação das demais penalidades cabíveis, por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

**3.** Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 11.1, de 1% a 30% do valor do Contrato.

**4.** Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 11.1, de 1% a 30% do valor do Contrato.

**5.** Para infração descrita na alínea "b" do subitem 11.1, a multa será de 1% a 30% do valor do Contrato.

**6**. Para infrações descritas na alínea "d" do subitem 11.1, a multa será de 1% a 30% do valor do Contrato.

**7.** Para a infração descrita na alínea "a" do subitem 11.1, a multa será de 1% a 30% do valor do Contrato, ressalvadas as seguintes infrações:

a) Quando se tratar de inexecução parcial acompanhada de justificativa aceita pela Administração, desde que não comprometa o interesse público ou a imponha risco à vida ou a serviços essênciais.

**11.3** A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Município de Santana de Parnaíba (art. 156, §9º, da Lei nº 14.133, de 2021).

**11.3.1.** Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

**11.3.2.** Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contados da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).

**11.3.3.** Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Município de Santana de Parnaíba, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

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

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

**11.5** Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

**a)** a natureza e a gravidade da infração cometida;

**b)** as peculiaridades do caso concreto;

**c)** as circunstâncias agravantes ou atenuantes;

**d)** os danos que dela provierem para o Contratante;

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

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

**11.7** A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

**11.8** O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

**11.9** As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

**11.10** Os débitos do contratado para com o Município de Santana de Parnaíba, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com esta municipalidade.

## CLÁUSULA XII – DA EXTINÇÃO CONTRATUAL

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

**12.1.1** O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

**12.1.2** A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

**12.1.3** Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

**12.2** O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

**12.2.1** Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

**12.2.2** A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

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

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

**12.3.1** Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

**12.3.2** Relação dos pagamentos já efetuados e ainda devidos;

**12.3.3** Indenizações e multas.

**12.4** A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

**12.5** O contrato poderá ser extinto caso se constate que o contratado 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 licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

## CLÁUSULA XIII – DOTAÇÃO ORÇAMENTÁRIA

**13.1** As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral do Município, na dotação abaixo discriminada:

**13.1.1** Gestão/Unidade: **Secretaria Municipal de Tecnologia da Informação - SMTI**

**13.1.2** Fonte de Recursos: **Tesouro Municipal**

**13.1.3** Função Programática: **0209-3.3.90.40-0412200152026 – SMTI – RESERVA Nº 2440/2024**

## CLÁUSULA XIV – DOS CASOS OMISSOS

**14.1** Os casos omissos serão decididos pela contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos e, no que couberem, as disposições do Decreto Municipal nº 4.990 de 28 de Dezembro de 2023.

## CLÁUSULA XV – ALTERAÇÕES

**15.1** Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021;

**15.2** A contratada é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato;

**15.3** As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 01 (um) mês (art. 132 da Lei nº 14.133, de 2021);

**15.4** Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

**CLÁUSULA XVI – PUBLICAÇÃO**

**16.1** Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021 e ao art. 8º, §2º, da Lei n. 12.527, de 2011.

**CLÁUSULA XVII – FORO**

**17.1** Fica eleito o Foro da Comarca de Santana de Parnaíba, Estado de São Paulo, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

**CLÁUSULA XVIII – DOS DADOS DO RESPONSÁVEL PELO AJUSTE**

**18.1** Para informar eletronicamente todos os processos de licitação via Sistema AUDESP (conforme os critérios previstos no Comunicado GP 14/2016, publicado no DOE de 24/06/2016), em atendimento às novas exigências do Tribunal de Contas do Estado de São Paulo, seguem os dados do responsável pelo ajuste:

**RESPONSÁVEL PELO AJUSTE/CONTRATADA:**

Nome:_____

Cargo:_____

CPF:_____

Data de nascimento: _____

E-mail particular: _____

E-mail profissional: _____

**GESTOR DO ÓRGÃO/ENTIDADE:**

Nome: _____

Cargo:_____

CPF: _____ RG: _____

Data de Nascimento: ____/____/_____

Endereço residencial completo: _____

E-mail institucional _____

E-mail pessoal:_____

Telefone(s):_____

Assinatura:_____

**CLÁUSULA XIX - DO CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS**

**19.1** É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

**19.2** As partes se comprometem a manter sigilo e confidencialidade de todas as informações - em especial os dados pessoais e os dados pessoais sensíveis - repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual.

**19.3** As partes responderão administrativa e judicialmente caso causarem danos patrimoniais, morais, individuais ou coletivos, aos titulares de dados pessoais repassados em decorrência da execução contratual, por inobservância à Lei Geral de Proteção de Dados.

**19.4** Em atendimento ao disposto na Lei Geral de Proteção de Dados, o **CONTRATANTE**, para a execução do serviço objeto deste contrato ou instrumento análogo, tem acesso a dados pessoais dos representantes da **CONTRATADA**, tais como: número do CPF e do RG, endereços eletrônico e residencial, e cópia do documento de identificação entre outros que possam ser exigidos para a execução contratual.

**19.5** A **CONTRATADA** declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo **CONTRATANTE**.

**19.6** A **CONTRATADA** fica obrigada a comunicar ao **CONTRATANTE** em até 24 (vinte e quatro) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados.

**CLÁUSULA XX – CONSIDERAÇÕES FINAIS**

**20.1** 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;

**20.2** E, por estarem assim justos e contratados, firmam as partes este instrumento em 03 (três) vias de igual teor, na presença das duas testemunhas adiante identificadas.

Santana de Parnaíba, ... de.....de 2024.

***PELA PREFEITURA***

***Nome:***_____

***Cargo:***_____

***CPF:***_____

***Data de nascimento:*** _____

***E-mail particular:***_____

***E-mail profissional:***_____

***PELA CONTRATADA***

***Nome:***_____

***Cargo:***_____

***CPF:***_____

***Data de nascimento:*** _____

***E-mail particular:***_____

***E-mail profissional:***_____

***TESTEMUNHAS***

***NOME:*** ***NOME:***

***RG.:*** ***RG .:***

***LC-01 - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO***

CONTRATANTE: _____

CONTRATADO: _____

CONTRATO Nº (DE ORIGEM):_____

OBJETO: _____

ADVOGADO (S)/ Nº OAB/email: (*)_____

Pelo presente TERMO, nós, abaixo identificados:

**1. Estamos CIENTES de que:**

a) o ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) as informações pessoais dos responsáveis pela contratante estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP – CadTCESP", nos termos previstos no Artigo 2º das Instruções nº01/2020, conforme "Declaração(ões) de Atualização Cadastral" anexa (s);

e) é de exclusiva responsabilidade do contratado manter seus dados sempre atualizados.

**2. Damo-nos por NOTIFICADOS para:**

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

**LOCAL e DATA:** _____

**AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:**

Nome: _____

Cargo:_____

CPF: _____

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

Nome: _____

Cargo:_____

CPF: _____

Assinatura: _____

**RESPONSÁVEIS QUE ASSINARAM O AJUSTE:**

**Pelo contratante:**

Nome: _____

Cargo:_____

CPF: _____

Assinatura: _____

**Pela contratada:**

Nome: _____

Cargo:_____

CPF: _____

Assinatura: _____

**ORDENADOR DE DESPESAS DA CONTRATANTE:**

Nome: _____

Cargo:_____

CPF: _____

Assinatura: _____

(*) Facultativo. Indicar quando já constituído, informando, inclusive, o endereço eletrônico.