PROCESSO	**Nº 13202/2026**
OBJETO	Contratação através de sistema de registro de preços objetivando a formalização de ATA com o vencedor do certame, visando a contratação de Solução de Cybersegurança para servidores, estações de trabalho e demais sensores de rede com gerenciamento da superfície de risco e microsegmentação de aplicações com visibilidade de conexões e contenção da rede, para a infraestrutura da SEMIT, na modalidade de subscrição de licença, incluindo suporte técnico no regime 24x7 (vinte e quatro horas por dia, sete dias por semana) e garantia de atualização das versões pelo período de 24 meses, contemplando também, instalação, configuração e treinamento de acordo com as especificações técnicas mínimas e detalhamentos consignados neste Termo de Referência (TR) e seus anexos, com a conveniência e necessidade da Prefeitura Municipal de Salvador – PMS, conforme as especificações, quantitativas e qualitativas e todas as demais condições gerais discorridas neste Termo de Referência (TR).
TIPO DE LICITAÇÃO	MENOR PREÇO
MODO DE DISPUTA	ABERTO E FECHADO
INICIO ACOLHIMENTO DAS PROPOSTAS	DATA: 25/05/2026 HORA: 08:00 – HORÁRIO DE BRASÍLIA
INÍCIO DA SESSÃO PÚBLICA	DATA: 26/05/2026 HORA: 10:00 – HORÁRIO DE BRASÍLIA LOCAL: https://licitacoes-e2.bb.com.br/aop-inter-estatico
TELEFONE CNPJ **E-MAIL**	(71) 3202-4225 13.927.801/0035-98 copel.semit@salvador.ba.gov.br
PREGOEIRO	Larissa da Silva Macedo

EDITAL DE PREGÃO ELETRÔNICO Nº 003/2026 SISTEMA DE REGISTRO DE PREÇOS SECRETARIA DE INOVAÇÃO E TECNOLOGIA DE SALVADOR

A **PREFEITURA MUNICIPAL DE SALVADOR**, por intermédio da Secretaria Municipal de Inovação e Tecnologia – SEMIT, inscrita no CNPJ sob nº 13.927.801/0035-98, levam ao conhecimento dos interessados que realizará licitação na modalidade PREGÃO ELETRÔNICO, tipo menor preço global, autorizada no processo nº 13202/2026 – SEMIT, nos termos da Lei nº 14.133, de 1º de abril de 2021, e posteriores dispositivos relacionados, bem como nos termos das condições e exigências estabelecidas neste instrumento convocatório e anexos, conforme abaixo informado.

As quantidades constantes no Termo de Referência são estimativas de consumo, não se obrigando a PREFEITURA MUNICIPAL DE SALVADOR à contratação.

Modalidade: Pregão Eletrônico: Registro de Preços **Critério de Julgamento:** Menor Preço Global **Formatação:** Eletrônica

Endereço: https://licitacoes-e2.bb.com.br/aop-inter-estatico

Modo de disputa: Aberto e Fechado

1 DO OBJETO

1.1 Contratação através de sistema de registro de preços objetivando a formalização de ATA com o vencedor do certame, visando a contratação de Solução de Cybersegurança para servidores, estações de trabalho e demais sensores de rede com gerenciamento da superfície de risco e microsegmentação de aplicações com visibilidade de conexões e contenção da rede, para a infraestrutura da SEMIT, na modalidade de subscrição de licença, incluindo suporte técnico no regime 24x7 (vinte e quatro horas por dia, sete dias por semana) e garantia de atualização das versões pelo período de 24 meses, contemplando também, instalação, configuração e treinamento de acordo com as especificações técnicas mínimas e detalhamentos consignados neste Termo de Referência (TR) e seus anexos, com a conveniência e necessidade da Prefeitura Municipal de Salvador – PMS, conforme as especificações, quantitativas e qualitativas e todas as demais condições gerais discorridas neste Termo de Referência (TR).

1.2 A presente licitação será realizada na modalidade de pregão eletrônico, com sistema de registro de preço, de acordo com o arrimado pelo art. 6º, incisos XLI e XLV; art. 28, inciso I; art. 29, parágrafo único, e art. 82, todos da Lei n.º 14.133/2021, bem como no Decreto Municipal n.º 38.051/2023, considerando a oportunidade de maior concorrência e competitividade aos interessados, a fim de oportunizar, igualmente, maior vantajosidade e economicidade ao ente público ordenador na escala de preços a serem ofertados, bem como pela oportunidade de descentralização operacional da Secretaria de Inovação e

Tecnologia de Salvador, viabilizando efetividade para concomitância da execução.

1.3 O critério de julgamento adotado será o menor preço, nos termos do art. 6º, inciso XLI, da Lei n.º 14.133/2021, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2 DAS DESPESAS E ÓRGÃOS PARTICIPANTES

2.1 As despesas decorrentes da execução da presente licitação correrão à conta dos recursos consignados ao orçamento dos órgãos indicados abaixo, do presente exercício, devidamente ajustadas nas dotações do exercício subsequente, impondo-se sempre que seja providenciada a prévia dotação orçamentária e, se cabível, o respectivo pré-empenho antes da celebração de qualquer contratação a ser efetivada em decorrência da presente licitação.

2.2 Serão participantes os órgãos e entidades da Administração Direta Municipais da Prefeitura Municipal de Salvador – PMS.

2.2.1 Secretaria do Governo – SEGOV

2.2.2 Gabinete do Vice-Prefeito – GABVP

2.2.3 Controladoria Geral do Município de Salvador – CGM

2.2.4 Procuradoria Geral do Município do Salvador – PGMS

2.2.5 Casa Civil

2.2.6 Secretaria Municipal da Comunicação – SECOM

2.2.7 Secretaria Municipal de Gestão – SEMGE

2.2.8 Secretaria Municipal de Inovação e Tecnologia – SEMIT

2.2.9 Secretaria Municipal da Fazenda – SEFAZ

2.2.10 Secretaria Municipal de Desenvolvimento Urbano – SEDUR

2.2.11 Secretaria Municipal de Sustentabilidade, Resiliência, Bem-estar e Proteção Animal– SECIS

2.2.12 Secretaria Municipal de Cultura e Turismo – SECULT

2.2.13 Secretaria Municipal de Desenvolvimento Econômico, Emprego e Renda – SEMDEC

2.2.14 Secretaria Municipal da Educação – SMED

2.2.15 Secretaria Municipal da Saúde – SMS

2.2.16 Secretaria Municipal de Promoção Social, Combate à Pobreza, Esportes e Lazer – SEMPRE

2.2.17 Secretaria Municipal de Reparação – SEMUR

2.2.18 Secretaria Municipal de Políticas para Mulheres, Infância e Juventude – SPMJ

2.2.19 Secretaria Municipal de Infraestrutura e Obras Públicas – SEINFRA

2.2.20 Secretaria Municipal de Manutenção da Cidade – SEMAN

2.2.21 Secretaria Municipal de Mobilidade – SEMOB

2.2.22 Defesa Civil de Salvador – CODESAL

2.2.23 Fundação Cidade Mãe – FCM

2.2.24 Fundação Gregório de Matos – FGM

2.2.25 Fundação Mário Leal Ferreira – FMLF

2.2.26 Guarda Civil Municipal – GCM

2.2.27 Superintendência de Trânsito de Salvador – TRANSALVADOR

2.2.28 Superintendência de Obras Públicas – SUCOP

2.2.29 Agência Reguladora e Fiscalizadora dos Serviços Públicos de Salvador – ARSAL

2.3 O órgão gerenciador será a Secretaria Municipal de Inovação e Tecnologia – SEMIT.

2.4 Fica facultado ao Município do Salvador, permitir durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal que não participaram do procedimento de IRP, poderão aderir à ata de registro de preços na condição de não participantes, desde que devidamente justificada a vantagem e com anuência do órgão gerenciador.

2.5 As contratações que trata o item anterior não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes (§ 4º do artigo 86, da Lei n.º 14.133/2021).

2.6 O órgão gerenciador somente poderá autorizar adesão à ata após a primeira aquisição ou contratação por órgão integrante da ata, exceto quando, justificadamente, não houver previsão no edital para aquisição ou contratação pelo órgão gerenciador.

2.7 Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

2.8 Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.

3 DA PARTICIPAÇÃO NA LICITAÇÃO

3.1 Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Compras eletrônico do Banco do Brasil Licitações.

3.1.1 Os interessados deverão atender às condições exigidas no cadastramento no Sistema de Compras eletrônico indicado no caput, até o terceiro dia útil anterior à data prevista para recebimento das propostas.

3.2 O licitante se responsabiliza 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.

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

3.4 A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

3.5 Será concedido tratamento favorecido para as Microempresas - ME e Empresas de Pequeno Porte - EPP, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133/2021, para o agricultor familiar, o produtor rural pessoa física e para o Microempreendedor Individual - MEI, nos limites previstos da Lei Complementar nº 123/2006.

3.5.1 A obtenção do benefício a que se refere o item anterior fica limitada às Microempresas - ME e às Empresas de Pequeno Porte - EPP que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como Empresa de Pequeno Porte – EPP.

3.6 Não poderá disputar esta licitação:

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

3.6.2 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;

3.6.3 Técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

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

3.6.5 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;

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

3.6.7 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;

3.6.8 Agente público do órgão ou entidade licitante;

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

3.6.10 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 n.º 14.133/2021.

3.7 O impedimento de que trata o subitem 3.6.4 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.

3.8 A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem o subitem 3.6.2 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.

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

3.9 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.

3.10 A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

3.11 A vedação de que trata o subitem 3.6.8 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.

4 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

4.1 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.

4.2 No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema:

4.3.1 que 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;

4.3.2 que 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 (quatorze) anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição Federal;

4.3.3 que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.3.4 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.

4.4 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 14.133/2021.

4.5 O fornecedor enquadrado como microempresa - ME, empresa de pequeno porte - EPP ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123/2006, 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 nº 14.133/2021.

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

4.6 A falsidade da declaração de que trata os itens 4.4 e 4.6 sujeitará o licitante às sanções previstas na Lei nº 14.133/2021, e neste Edital.

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

4.8 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:

I. 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

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

4.9 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:

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

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

4.10 O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 4.9, incisos I e II, 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.

4.11 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.

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

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

4.13.1 Valor unitário e total para cada item ou lote de itens, em moeda corrente nacional;

4.13.2 Marca de cada item ofertado;

4.13.3 Fabricante de cada item ofertado;

4.13.4 Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia, número do registro ou inscrição do bem no órgão competente, quando for o caso;

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

4.15 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens ou serviços.

4.16 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.

4.17 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 12 (doze) meses.

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

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

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

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

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

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

5.2 Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação até a abertura da sessão pública.

5.2.1 Será desclassificada a proposta que identifique o licitante.

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

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

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

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

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

5.5.1 O lance deverá ser ofertado pelo valor global do lote.

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 poderá oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no edital.

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

5.9 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 1% (um porcento) do valor estimado.

5.10 O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 (quinze) segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.11 O sistema adotado para o envio de lances no pregão eletrônico será no modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1 A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, o que transcorrerá o período de tempo de até 10 (dez) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2 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) superior àquela, possam ofertar um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.3 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.

5.11.4 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 3 (três), oferecer um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

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

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

5.13 Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo Pregoeiro.

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

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

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

5.17 Havendo apenas uma oferta, esta poderá ser aceita, desde que atenda todas as condições do instrumento convocatório e seu preço seja compatível com o valor estimado para a contratação e dentro da realidade do mercado.

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

5.18.1 Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor

proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

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

5.18.3 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.

5.18.4 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.

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

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

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

II. Avaliação do desempenho contratual prévio dos licitantes;

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

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

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

i. 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;

ii. Empresas brasileiras;

iii. Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no país;

iv. Empresas que comprovem a prática de mitigação, nos termos da lei nº 12.187/2009.

5.21 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.

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

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

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

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

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

5.22 Após o envio da proposta adequada ao último lance ofertado pelo licitante mais bem classificado, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6 DA FASE DO JULGAMENTO

6.1 Encerrada a etapa de disputa, 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, na legislação correlata e no item 3.7 deste Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, nos termos do art. 156 da Lei nº 14.133/2021, e mediante a consulta aos cadastros previstos no art.91 § 4º da referida Lei e aos cadastros utilizados pelo Município do Salvador:

6.2 Atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.3 Na hipótese de o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às microempresas - ME e as empresas de pequeno porte - EPPs, o pregoeiro verificará se o licitante faz jus ao benefício, em conformidade com os itens 3.5.1 e 4.6 deste Edital..

6.4 o 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 nos artigos 29 ao 35 do Decreto nº 36.784 de 30 de março de 2023.

6.5 Será desclassificada a proposta vencedora que:

6.5.1 contiver vícios insanáveis;

6.5.2 não obedecer às especificações técnicas contidas no Termo de Referência, neste Edital e seus Anexos;

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

6.5.4 não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

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

6.6 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;

6.7 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.

6.8 Não será causa de desclassificação as irregularidades formais que não afetem o conteúdo das propostas ou não impeçam o seu entendimento e que não comprometam os interesses da Administração.

6.8.1 Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta, podendo ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço, e que se limite a sanar erros ou falhas que não alterem a substância das propostas;

6.8.2 Serão objeto de saneamento, mediante ato motivado do Pregoeiro, os erros materiais irrelevantes, considerados aqueles cuja ocorrência não comprometam a Administração e a idoneidade do documento ou a perfeita compreensão do conteúdo da proposta.

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

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

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

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

6.13 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 DO BENEFÍCIO ÀS MICROEMPRESAS E ÀS EMPRESAS DE PEQUENO PORTE

7.1 A obtenção de benefícios previstos dos artigos 42 a 49 da Lei Complementar nº 123/2006 fica limitado às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda que não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, devendo o licitante apresentar declaração de observância desse limite para fins de habilitação.

7.2 Após a fase de lances, se a proposta mais bem classificada não tiver sido apresentada por microempresa ou empresa de pequeno porte apta a usufruir dos benefícios e se houver proposta de microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior à proposta mais bem classificada, proceder-se-á da seguinte forma:

7.2.1 A Microempresa - ME ou a Empresa de Pequeno Porte - EPP mais bem classificada poderá, no prazo de 5 (cinco) minutos, apresentar proposta de preço inferior à do licitante mais bem classificado e, se atendidas as exigências deste Edital, ser adjudicatária;

7.2.2 Não sendo adjudicatária a Microempresa - ME ou Empresa de Pequeno Porte - EPP mais bem classificada na forma do inciso anterior, e havendo outros licitantes que se enquadrem na condição prevista no caput deste item, estes serão convocados, na ordem classificatória, para o exercício do mesmo direito;

7.2.3 O convocado que não apresentar proposta dentro do prazo de 5 (cinco) minutos, controlado pelo sistema eletrônico, decairá do direito previsto nos arts. 44 e 45 da Lei Complementar nº 123/2006.

7.3 Na hipótese de não adjudicação nos termos previstos nesta cláusula, o procedimento licitatório prosseguirá com os demais licitantes.

7.4 As disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123/2006 não se aplicam:

7.4.1 No caso de licitação para aquisição de bens ou contratação de serviços em geral, ao item cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte;

7.4.2 No caso de contratação de obras e serviços de engenharia, às licitações cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

8 DA NEGOCIAÇÃO

8.1 O pregoeiro deverá encaminhar contraproposta diretamente ao licitante que tenha apresentado o lance mais vantajoso, observados o critério de julgamento e o valor estimado para a contratação.

8.2 A negociação será realizada por meio do sistema eletrônico e poderá ser acompanhada pelos demais licitantes.

8.3 Após a negociação a proposta que apresentar valor superior ao estabelecido em orçamento estimado contido neste Edital será desclassificada.

9 DA ACEITABILIDADE DA PROPOSTA

9.1 Encerrada a etapa competitiva de lances, exercido o direito de preferência e concluída a negociação, o pregoeiro iniciará os procedimentos necessários à aceitabilidade da proposta de melhor preço e verificará a conformidade das especificações técnicas com as exigências contidas neste Edital e a compatibilidade do preço ofertado com o valor estimado para a contratação, podendo solicitar, se necessário, a planilha de composição de custos adequada ao lance equivalente à proposta de melhor preço no prazo estipulado no chat durante a sessão.

9.2 Se o mesmo licitante vencer tanto a cota reservada quanto a cota principal, a contratação ocorrerá em um único instrumento e pelo menor preço obtido.

9.2.1 No caso de não haver vencedor para a cota reservada, esta poderá ser adjudicada ao vencedor da cota principal ou, diante de sua recusa, aos licitantes remanescentes, desde que pratiquem o preço do primeiro colocado da cota principal.

9.2.2 No caso de não haver vencedor para a cota principal, esta poderá ser adjudicada ao vencedor da cota reservada ou, diante de sua recusa, aos licitantes remanescentes, desde que pratiquem o preço do primeiro colocado da cota reservada.

9.3 Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

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

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

9.4 Serão desclassificadas, da mesma forma, as propostas que não atenderem às demais condições estabelecidas neste Edital e anexos.

9.5 O pregoeiro poderá solicitar manifestação técnica dos outros setores do Órgão ou Entidade a fim de subsidiar sua decisão e da assessoria jurídica quando existir dúvida jurídica.

9.6 Não se considerará qualquer oferta ou vantagem não prevista neste Edital, inclusive financiamentos subsidiados ou a fundo perdido.

10 DA HABILITAÇÃO

10.1 Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade de o licitante cumprir com o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos artigos 62º a 70º da Lei nº 14.133/2021.

10.2 A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo Certificado de Registro Cadastral – CRC, expedido pelo Município de Salvador.

10.3 Os documentos exigidos para habilitação deverão ser enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, contadas a partir da solicitação do pregoeiro no sistema, podendo esse prazo ser prorrogado por igual período, mediante solicitação justificada da licitante apresentada antes do seu término.

10.4 Quando permitida a participação de empresas estrangeiras que não funcionem no País, estas deverão apresentar documentos equivalentes, na forma de regulamento emitido pelo Poder Executivo Federal.

10.5 Para habilitação nesta licitação será exigida a documentação, anexada preferencialmente por grupos: Habilitação jurídica, Habilitação fiscal, social e trabalhista, Qualificação Técnica, Qualificação econômico-financeira e outros documentos.

DOCUMENTAÇÃO RELATIVA À HABILITAÇÃO JURÍDICA:

10.5.1 **Pessoa física:** Cédula de identidade - (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional.

10.5.2 **Empresário individual:** Inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede.

10.5.3 **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor.

10.5.4 **Sociedade Empresária, Sociedade Limitada Unipessoal - SLU ou sociedade identificada como Empresa Individual de Responsabilidade Limitada - EIRELI:** Inscrição do ato constitutivo; Estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores.

10.5.5 **Sociedade empresária estrangeira:** Portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa do Departamento Nacional de Registro Empresarial e Integração - DREI/ME n.º 77, de 18 de março de 2020.

10.5.6 **Sociedade simples:** Inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores.

10.5.7 **Filial, sucursal ou agência de sociedade simples ou empresária:** Inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.

10.5.8 **Sociedade cooperativa:** Ata de fundação; Estatuto social e a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede; Registro na Organização das Cooperativas Brasileiras ou na entidade estadual, se houver, conforme art. 107º da Lei nº 5.764/1971.

10.5.9 **Agricultor familiar:** Declaração de Aptidão ao Pronaf - DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 4º, §2º do Decreto nº 10.880, de 2 de dezembro de 2021.

10.5.10 **Produtor Rural**: Matrícula no Cadastro Específico do INSS - CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa da Receita Federal do Brasil - RFB nº 2110, de 17 de outubro de 2022.

DOCUMENTAÇÃO RELATIVA À HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA;

10.5.11 Inscrição no Cadastro de Pessoas Físicas - CPF ou no Cadastro Nacional da Pessoa Jurídica - CNPJ;

10.5.12 Inscrição no Cadastro de contribuintes estadual e/ou municipal, se houver.

10.5.13 O cadastro de contribuinte estadual e/ou municipal deverá ser relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.5.14 Certidão de regularidade perante a Fazenda federal, estadual e municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

10.5.15 Certidão de regularidade relativa à Seguridade Social e ao FGTS;

10.5.16 Certidão de regularidade perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas. (Lei nº 12.440/2011);

10.5.17 Declaração de cumprimento ao disposto no inciso XXXIII do art. 7º da Constituição Federal.

10.5.18 Certidão Negativa no CADIN/Salvador conforme determina artigo 34º da Lei Municipal n° 8.421/2013 e no art. 3º do Decreto municipal n° 24.419/2013.

DOCUMENTAÇÃO RELATIVA À QUALIFICAÇÃO ECONÔMICA E FINANCEIRA;

10.5.19 Balanço patrimonial;

10.5.20 Demonstrações do resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais;

10.5.21 Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante;

10.5.22 O balanço patrimonial e as demonstrações contábeis deverão ser apresentados mediante cópia do Termo de Abertura e do Termo de Encerramento assinados pelo contador responsável e pelo representante legal da empresa;

10.5.23 Em se tratando de Sociedade por Ações - S/A, deverá ser apresentada a publicação em Órgão de Imprensa Oficial;

10.5.24 As sociedades com menos de 01 (um) ano de existência, que ainda não tenham balanço de final de exercício, deverão apresentar demonstrações contábeis envolvendo seus direitos, obrigações e patrimônio líquido relativo ao período de sua existência;

10.5.25 O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

10.5.26 Certidão expedida por país estrangeiro deverá atestar que a empresa estrangeira não se encontra em processo de falência, concordata ou outro instituto assemelhado que possa de qualquer forma comprometer o fiel cumprimento das obrigações, devendo ser observada a respectiva data de vigência.

10.5.27 A proposta e quaisquer documentos deverão ser apresentados em português, idioma em que também será redigido o Contrato.

10.5.28 Serão aceitos documentos em outros idiomas, desde que acompanhados de tradução para o idioma português, firmada por tradutor juramentado e autenticados por autoridade consular brasileira, caso em que tal tradução prevalecerá sobre os originais;

DOCUMENTAÇÃO RELATIVA À QUALIFICAÇÃO TÉCNICA;

10.5.29 A empresa Licitante deverá apresentar atestado(s) de Capacidade Técnica, expedido(s) por pessoa jurídica de direito público ou privado, comprovando aptidão para a execução que a mesma tenha executado serviço semelhante e compatível com solução de cibersegurança com visibilidade e proteção de ameaças na rede.

10.5.30 Os atestados deverão ser impressos em papel timbrado, com nome e telefone de contato dos responsáveis pela informação atestada, não sendo aceitas declarações genéricas, devendo ainda atestar a satisfação com o serviço ofertado pela PROPONENTE.

10.5.31 A CONTRATANTE se reserva o direito de conferir as informações prestadas pelas empresas emitentes dos atestados, através de consultas e visitas, bem como a disponibilidade de equipamentos solicitados junto à PROPONENTE.

10.5.32 A PROPONENTE deverá apresentar os seguintes documentos:

10.5.33 Indicação de site na WEB para transferência de arquivos de configuração (manuais e atualizações de firmware);

10.5.34 Prospecto com as características técnicas de todos os componentes dos equipamentos, incluindo especificação de marca, modelo e outros elementos que, de forma inequívoca, identifiquem e comprovem as configurações cotadas, possíveis expansões e upgrades, através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em websites dos fabricantes na Internet, em que conste o respectivo endereço eletrônico;

10.5.35 Deve ser apresentada uma planilha de comprovação técnica para todas as especificações exigidas neste termo de referência através de documento oficial do fabricante, pagina e texto de comprovação.

10.5.36 Indicação exata do modelo de equipamento ofertado, no Sistema Eletrônico de Disputas e na Proposta de Preços, sendo os respectivos catálogos obrigatoriamente de domínio público, ou seja, deverão estar publicados no website do fabricante, comprovando todos os recursos e funcionalidades mínimas exigidas para os equipamentos que irão integrar as características técnicas solicitadas no Anexo A.

10.5.37 O não cumprimento dos quaisquer dos requisitos de habilitação, ensejará na automática inabilitação da proponente.

DEMAIS CRITÉRIOS PARA QUALIFICAÇÃO;

10.5.38 Os documentos relativos à habilitação jurídica apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

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

10.5.40 Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, caso exigidos, e no caso daqueles documentos

que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

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

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

10.5.43 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.

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

10.5.45 O pregoeiro poderá consultar sítios oficiais de órgãos e entidades emissores de certidões para verificar as condições de habilitação dos licitantes.

10.5.46 Havendo a necessidade de envio de documentos para a confirmação daqueles exigidos neste Edital e já apresentados, ou, ainda, de envio de documentos não juntados, mas que comprovem que na data da apresentação da proposta o licitante atendia às condições de aceitabilidade da proposta e de habilitação, o licitante será convocado a encaminhá-los, via sistema eletrônico, no prazo fixado pelo pregoeiro, sob pena de desclassificação ou de inabilitação, prazo durante o qual a sessão não será suspensa.

10.5.47 Em se tratando de microempresa - ME ou empresa de pequeno porte - EPP, aplica-se o disposto no artigo 43, § 1º da Lei Complementar nº 123/2006.

10.5.48 A não regularização da documentação no prazo previsto na legislação mencionada no subitem anterior implicará decadência do direito à contratação, sem prejuízo das sanções previstas neste Edital, e facultará ao pregoeiro convocar os licitantes remanescentes, na ordem de classificação.

10.5.49 Se a proposta for desclassificada ou, ainda, se o licitante não atender às exigências de habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este Edital.

10.5.50 O fornecedor enquadrado como Microempreendedor Individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123/2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

11 DO RECURSO

11.1 Caberá recurso em face de:

11.1.1 Julgamento das propostas;

11.1.2 Ato de habilitação ou inabilitação de licitante;

11.1.3 Anulação ou revogação da licitação.

11.2 Nos recursos de julgamento das propostas e de ato de habilitação ou inabilitação de licitante serão observadas as seguintes disposições:

11.2.1 A intenção de recorrer deverá ser manifestada imediatamente em até 10 (dez) minutos exclusivamente no sistema eletrônico, sob pena de preclusão, e o prazo para apresentação das razões recursais de 3 (três) dias úteis será iniciado a partir ato de habilitação ou inabilitação ou, na hipótese de adoção da inversão de fases prevista no §1º do art. 17º da Lei

nº 14.133/2021, da ata de julgamento;

11.2.2 A apreciação se dará em fase única.

11.3 Não será admitida intenção de recurso de caráter protelatório, fundada em mera insatisfação do licitante, ou baseada em fatos genéricos.

11.4 A ausência de manifestação imediata e motivada quanto a intenção de recorrer no prazo estabelecido, importará na decadência desse direito, autoriza a Administração a adjudicar o objeto a licitante vencedora.

11.5 O pregoeiro examinará a intenção de recurso, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema eletrônico.

11.6 O licitante que tiver sua intenção de recurso aceita deverá registrar as razões do recurso em campo próprio do sistema no prazo de 3 (três) dias úteis contados do término do julgamento das propostas ou do ato de habilitação ou inabilitação, ficando os demais licitantes, desde logo, intimados a apresentar contrarrazões, contados da disponibilização das razões do recurso no sistema, nos moldes do art. 165º da Lei nº 14.133/2021.

11.7 O não oferecimento de razões no prazo previsto implicará em não conhecimento do recurso.

11.8 As intenções de recurso não admitidas e os recursos rejeitados pelo pregoeiro serão a ele dirigidos, que, se não reconsiderar o ato ou a decisão no prazo de 3 (três) dias úteis, encaminhará o recurso com a sua motivação à autoridade superior, a qual deverá proferir sua decisão no prazo máximo de 10 (dez) dias úteis, contado do recebimento dos autos.

11.9 As razões e contrarrazões de recurso deverão ser enviados/anexados, exclusivamente, no sistema eletrônico.

11.10 O acolhimento do recurso implicará a invalidação apenas dos atos não suscetíveis de aproveitamento.

11.11 Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

11.12 O recurso terá efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

12 DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

12.1 Não havendo manifestação de recurso, o objeto deste pregão será adjudicado ao licitante vencedor.

12.2 Decididos os recursos eventualmente interpostos e constatada a regularidade dos atos procedimentais, a autoridade superior adjudicará o objeto licitado ao licitante vencedor homologando em seguida, o procedimento licitatório.

12.3 A homologação e a adjudicação do objeto desta licitação não implicarão direito à contratação.

13 DO INSTRUMENTO CONTRATUAL

13.1 Depois de homologado o resultado deste pregão, o licitante vencedor será convocado para, dentro do prazo de 5 (cinco) dias úteis, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital, assinar o instrumento contratual.

13.2 A exigência de garantia e/ou validade do produto obedecerá às previsões do Termo de Referência.

13.3 As contratações decorrentes dos itens de cota principal e de cota reservada ocorrerão inicialmente pelo menor preço, independentemente da qualificação da contratada.

13.4 Por ocasião da assinatura do instrumento contratual, será verificado no

Certificado de Registro Cadastral - CRC e em outros meios se o adjudicatário mantém as condições de habilitação.

14 DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

14.1 Comete infração administrativa, nos termos da Lei nº 14.133/2021, o Licitante que com dolo ou culpa:

14.1.1 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;

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

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

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

c) pedir para ser desclassificado quando encerrada a etapa competitiva; ou

d) deixar de apresentar amostra;

e) apresentar proposta ou amostra em desacordo com as especificações do Edital.

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

14.1.3.1 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.

14.1.4 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

14.1.5 Fraudar a licitação;

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

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

b) induzir deliberadamente a erro no julgamento;

c) apresentar amostra falsificada ou deteriorada;

14.1.7 Praticar atos ilícitos com vistas a frustrar os objetivos da licitação

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

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

14.2.1 Advertência;

14.2.2 Multa;

14.2.3 Impedimento de licitar e contratar;

14.2.4 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.

14.3 Na aplicação das sanções serão considerados:

14.3.1 A natureza e a gravidade da infração cometida;

14.3.2 As peculiaridades do caso concreto;

14.3.3 As circunstâncias agravantes ou atenuantes;

14.3.4 Os danos que dela provierem para a Administração Pública;

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

14.4 A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato ou empenho, a contar da comunicação oficial.

14.4.1 Para as infrações previstas nos subitens 14.1.1, 14.1.2 e 14.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

14.4.2 Para as infrações previstas no item 14.1.4 e 14.1.5, a multa será de 15% a 30% do valor do contrato licitado.

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

14.6 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.

14.7 A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas no item 14.1 incisos I, II e III, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública Municipal direta e indireta pelo prazo máximo de 3 (três) anos.

14.8 Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos subitens 14.1.4 a 14.1.8, bem como pelas infrações administrativas previstas nos subitens 14.1.1 a 14.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no § 5º do art. 156, da Lei n.º 14.133/2021.

14.9 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 subitem 14.1.3, 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. 58º §3º da Lei n. 14.133/2021.

14.10 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 pela Comissão de Cadastro e Avaliação de Fornecedores - COMPEC, da Secretaria Municipal de Gestão - SEMGE, 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.

14.11 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.

14.12 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.

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

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

15 DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

15.1 Até 3 (três) dias úteis antes da data fixada para a abertura da sessão pública, qualquer pessoa, física ou jurídica, poderá impugnar o ato convocatório deste pregão, por irregularidade na aplicação de Lei ou para solicitar esclarecimento sobre os seus termos, mediante petição, a ser enviada exclusivamente para o endereço: copel.semit@salvador.ba.gov.br

15.2 A comissão de licitação, auxiliada pelo setor técnico competente, decidirá sobre a impugnação do certame.

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

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

15.5 Acolhida a impugnação do certame, será designada nova data para sua realização, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

15.6 As impugnações serão enviadas eletronicamente em formato Portable Document Format - PDF, com tamanho máximo de 5 (cinco) megabytes.

15.7 Os pedidos de esclarecimento deverão ser enviados exclusivamente via internet.

15.8 As respostas às impugnações e aos esclarecimentos solicitados serão disponibilizadas no sistema eletrônico em até 3 (três) dias úteis, contados do recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame.

16 DA PROVA DE CONCEITO

16.1 Não haverá prova de conceito.

17 DA ANTICORRUPÇÃO

17.1 Os licitantes e contratados devem observar o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos desta cláusula, definem-se as seguintes práticas:

17.1.1 prática corrupta: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

17.1.2 prática fraudulenta: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

17.1.3 prática colusiva: esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

17.1.4 prática coercitiva: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato.

17.1.5 prática obstrutiva:

a) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista deste Edital;

b) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

17.2 Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, inclusive declarando-a inelegível, indefinidamente ou por prazo determinado, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, colusivas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

17.3 Considerando os propósitos das cláusulas acima, o licitante vencedor, como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos, contas e registros relacionados à licitação e à execução do contrato.

18 DA ATA DE REGISTRO DE PREÇO

18.1 A ata de registro de preços para execução do objeto desta licitação, terá validade de 01 (um) ano, contado a partir da data de sua publicação na imprensa oficial e poderá ser prorrogada por igual período desde que comprovado o preço vantajoso ao Município, nos termos do art. 84º, da Lei N.º 14.133/2021. Caso a ata de registro de preços ultrapasse o exercício, deverá a administração atualizar, por meio de apostila e de forma unilateral, as disposições que assim se permitirem, inclusive a própria rubrica orçamentária da lei em vigor.

18.2 Homologado o resultado da licitação, o licitante mais bem classificado terá prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

18.3 O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

18.3.1 A solicitação seja devidamente justificada e apresentada dentro do prazo.

18.3.2 A justificativa apresentada seja aceita pela Administração.

18.4 Serão formalizadas tantas Atas de Registro de Preços quantas forem necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais.

18.5 O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.

18.6 A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

19 DA FORMAÇÃO DO CADASTRO DE RESERVA DA ATA DE REGISTRO DE PREÇOS

19.1 Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:

19.1.1 dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

19.1.2 dos licitantes que mantiverem sua proposta original.

19.2 Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.

19.3 Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original.

19.4 A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

19.4.1 quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou

19.4.2 quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28º e art. 29º do Decreto nº 11.462/23.

19.5 Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

19.5.1 Convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

19.5.2 Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

20 A FORMALIZAÇÃO E EXECUÇÃO DA ATA DE COMPROMISSO DE FORNECIMENTO

20.1 A execução da ata de registro de preços e dos contratos administrativos se regerá pelo estabelecido nos artigos 115º a 123º da Lei 14.133/2021, bem como pelos regulamentos próprios municipais editados e vigentes, parte integrante deste Edital e demais atos subsequentes.

20.2 A ata de registro de preços a ser firmada entre a SEMIT e a licitante vencedora, obedecerá à minuta sob Anexo IV deste Edital, dentro do prazo convocatório estabelecido neste Edital.

20.3 Antes de formalizar a ata de registro de preços, a Administração deverá verificar a regularidade fiscal do contratado, consultar o Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e o Cadastro Nacional de Empresas Punidas (Cnep), emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo.

20.4 A desistência do órgão ou entidade promotora da licitação de contratar com a licitante mais bem classificada não lhe confere o direito à indenização ou reembolso de qualquer espécie.

21 DO RECEBIMENTO DO MATERIAL DO REGISTRO DE PREÇO

21.1 O recebimento do objeto da Ata de Registro de Preço se dará pela Prefeitura Municipal de Salvador, consoante Art. 140º, da Lei 14.133/2021, e demais normas pertinentes.

21.2 Os responsáveis pelo atesto efetuarão vistoria no ato de entrega e avaliarão as condições dos produtos ou serviços prestados. Caso estas condições não sejam satisfatórias, ou estejam em desacordo com as especificações contidas no Termo de Referência, Anexo III deste Edital, o item poderá ser devolvido ou a prestação do serviço recusada, devendo ser substituída por outra, independente da aplicação das penalidades previstas.

21.3 Corre por conta da detentora da Ata, qualquer prejuízo causado ao produto em decorrência do transporte.

21.4 O objeto do presente certame, deverá estar de acordo com a solicitação do órgão gerenciador ou órgãos gerenciados da presente ATA, obedecendo o horário e o endereço indicado por estes, no prazo estipulado no Termo de Referência, devendo comunicar-se previamente com o fiscal do contrato para que este acompanhe a entrega.

21.5 Verificada a não conformidade das características do produto ou serviço, o detentor da Ata deverá promover as correções necessárias no prazo máximo fixado em Termo de Referência, sujeitando-se às penalidades previstas neste Edital.

21.6 A Nota Fiscal/Fatura deve, obrigatoriamente, ser entregue no órgão demandante, após a entrega do solicitado junto ao local designado pela mesma.

22 DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇO

22.1 O registro de preços será cancelado quando o fornecedor:

22.1.1 Descumprir as condições da ata de registro de preços;

22.1.2 Não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

22.1.3 Não aceitar reduzir o preço de contrato decorrente da ata, na hipótese deste se tornar superior àqueles praticados no mercado; ou;

22.1.4 Sofrer as sanções previstas nos incisos III ou IV do caput do art. 156º da Lei nº 14.133, de 1º de abril de 2021;

22.1.5 O cancelamento de registros nas hipóteses previstas nos incisos I, II e IV do caput será formalizado por despacho fundamentado.

22.2 O cancelamento do registro de preços também poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

22.2.1 Por razão de interesse público; ou

22.2.2 A pedido do fornecedor.

23 DISPOSIÇÕES FINAIS

23.1 Será divulgada ata da sessão pública no sistema eletrônico.

23.2 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.

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

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

23.5 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.

23.6 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.

23.7 À autoridade superior compete anular este pregão por ilegalidade, de ofício ou por provocação de qualquer pessoa, e revogar o certame por considerá-lo inoportuno ou inconveniente diante de fato superveniente, mediante ato escrito e fundamentado.

23.8 No julgamento das propostas e na fase de habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhe validade e eficácia para fins de classificação e habilitação.

23.9 É facultado ao pregoeiro ou à autoridade superior, em qualquer fase deste pregão, promover diligência destinada a esclarecer ou completar a instrução do processo, sendo vedada, ressalvados os casos previstos neste Edital, a inclusão posterior de informações ou de documentos que deveriam ter sido apresentados para fins de classificação e habilitação.

23.10 Caso os prazos definidos neste Edital não estejam expressamente indicados na proposta, eles serão considerados como aceitos pelos licitantes para efeitos de julgamento deste pregão.

23.11 Poderá ser solicitada tradução para a língua portuguesa, efetuada por tradutor juramentado, de documentos emitidos em língua estrangeira, que também deverão ser devidamente consularizados ou registrados em cartório de títulos e documentos.

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

23.13 Este pregão poderá ter a data de abertura da sessão pública alterada desde que motivado o ato do adiamento.

23.14 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.

23.15 Os dados pessoais decorrentes da execução deste Edital ficam, desde já,

autorizados pelos licitantes e respectivos representantes, inclusive a eventual vencedor do certame e contratado (s), à disponibilidade pública nos sítios oficiais de informação e publicidade, nos termos do art. 7º, inciso I, da Lei n.º 13.709, de 14 de agosto de 2018.

23.16 Os casos omissos serão decididos pelo Pregoeiro, Comissão de Contratação e/ou Equipe de Apoio, nos termos dos regulamentos municipais condizentes com a Lei n.º 14.133/2021, bem como nos termos das demais legislações em vigor e Princípios Gerais de Direito.

23.17 Até que esteja sendo amplamente utilizado o Portal Nacional de Contratações Públicas - PNCP, para fins de garantir a ampla publicidade, este Edital será divulgado na página eletrônica da Prefeitura Municipal do Salvador - PMS, no endereço eletrônico: compras.salvador.ba.gov.br, no portal compras.gov.br e em jornal local de grande circulação.

23.18 São partes integrantes deste Edital: ANEXO I – ORÇAMENTO ESTIMATIVO

ANEXO II – TERMO DE REFERÊNCIA E SEUS ANEXOS

ANEXO III - TERMO DE COMPROMISSO DE FORNECIMENTO ANEXO IV – MINUTA DE CONTRATO

ANEXO V - MODELO DE DECLARAÇÃO A SEREM APRESENTADAS JUNTAMENTE COM A PROPOSTA:

a) Declaração Negativa De Relação Familiar Ou Parentesco;

b) Declaração De Cumprimento Da Lei Geral De Proteção De Dados - Lei Nº 13.709/2018;

c) Declaração De Integralidade Dos Custos;

d) Declaração De Reserva De Cargos;

e) Declaração De Que Pode Usufruir Dos Benefícios De ME e EPP;

f) Declaração Para Qualificação Econômico-Financeira;

g) Declaração De Atendimento Ao Inciso XXXIII Do Art. 7º. Da Constituição Federal;

h) Declaração De Vistoria;

i) Declaração De Pleno Conhecimento Do Edital e Anexos;

j) Declaração De Contratos Firmados Com e Iniciativa Privada e a Administração Pública.

ANEXO VI – ATA DE REGISTRO DE PREÇOS

24 DO FORO

24.1 As questões decorrentes das previsões deste Edital que não possam ser dirimidas administrativamente serão processadas e julgadas na Justiça Estadual, no Foro da Comarca de Salvador, com exclusão de qualquer outro, por mais privilegiado que seja.

SECRETARIA MUNICIPAL DE INOVAÇÃO E TECNOLOGIA – SEMIT

PREGÃO ELETRÔNICO Nº 003/ 2026 ANEXO I - ORÇAMENTO ESTIMATIVO

PROCESSO: 13202/2026 MODALIDADE DE LICITAÇÃO:

NÚMERO DA LICITAÇÃO:

O **valor máximo estimado** para a presente contratação é de R$ 57.640.031,74 (cinquenta e sete milhões seiscentos e quarenta mil trinta e um reais e setenta e quatro centavos), resultante da pesquisa de mercado efetuada..

			TABELA MÉDIA	
ITEM	DESCRIÇÃO	QTD.	VALOR UNITÁRIO	VALOR TOTAL
Grupo 1 – Solução de Cybersegurança para Servidores, estações de trabalho com gerenciamento da superfície de risco				
1	Trend Micro Vision +B10:B16One Endpoint Security Pro, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	1500	R$ 1.669,33	R$ 2.503.995,00
2	Trend Micro Email and Collaboration Security, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	34.000	R$ 449,33	R$ 15.277.220,00
3	Trend Micro Deep Discovery Inspector – 4Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	4	R$ 1.434.956,75	R$ 5.739.827,00
4	Trend Micro TippingPoint Threat Protection System (TPS) 5Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	4	R$ 1.144.220,13	R$ 4.576.880,52
5	Trend Micro TippingPoint Threat Protection System (TPS) 10Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	3	R$ 1.831.899,97	R$ 5.495.699,91
6	Trend Micro Plataforma TrendAi Vision One – por 24 (vinte e quatro) meses.	500.000	R$ 7,46	R$ 3.730.000,00
7	Trend Micro Service One Complete (rede 4Gbps), por 24 (vinte e quatro) meses.	4	R$ 1.154.663,83	R$ 4.618.655,32
8	Trend Micro Service One Complete (endpoint), por 24 (vinte e quatro) meses.	1500	R$ 496,60	R$ 744.900,00
9	Network Packet Broker, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	2	R$ 335.108,67	R$ 670.217,34
10	Módulo mini-gbic SFP+ gigabit Ethernet Base-SR, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	40	R$ 2.269,33	R$ 90.773,20
11	Módulo mini-gbic SFP gigabit Ethernet 10GBASE-T, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	24	R$ 4.579,00	R$ 109.896,00
12	Funcionalidade de Descriptografia de Rede SSL/TLS em linha, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	2	R$ 425.167,00	R$ 850.334,00
13	Funcionalidade de Otimização de Cópia de Tráfego para Ferramentas, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	2	R$ 135.969,33	R$ 271.938,66
14	Gerência Centralizada - Network Packet Broker, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses.	1	R$ 82.674,17	R$ 82.674,17
15	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 1	1500	R$ 252,59	R$ 378.885,00
16	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 2	34.000	R$ 26,00	R$ 884.000,00
17	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 3	4	R$ 421,34	R$ 1.685,36
18	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 4	4	R$ 471,34	R$ 1.885,36
19	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 5	3	R$ 471,34	R$ 1.414,02
20	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 9	2	R$ 471,34	R$ 942,68
21	Treinamento oficial	15	R$ 15.197,88	R$ 227.968,20
Grupo 2 – Solução de Cybersegurança para Microsegmentação de aplicações com visibilidade de conexões e contenção da rede				
22	Solução de microssegmentação, visibilidade e proteção de Rede, baseada em Software, para controle de movimentação lateral em ambiente corporativo de servidores	1500	R$ 6.335,25	R$ 9.502.875,00
23	Solução de microssegmentação, visibilidade e proteção de Rede, baseada em Software, para controle de movimentação lateral em ambiente corporativos em Containers	50	R$ 25.582,00	R$ 1.279.100,00
24	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 22	1500	R$ 226,67	R$ 340.005,00
25	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 23	50	R$ 310,00	R$ 15.500,00
26	Treinamento oficial	15	R$ 16.184,00	R$ 242.760,00
VALOR TOTAL GLOBAL			R$ 57.640.031,74	

SECRETARIA MUNICIPAL DE INOVAÇÃO E TECNOLOGIA – SEMIT PREGÃO ELETRÔNICO Nº 003/ 2026

ANEXO II - TERMO DE REFERÊNCIA

1 OBJETO

1.0 Contratação através de sistema de registro de preços objetivando a formalização de ATA com o vencedor do certame, visando a contratação de Solução de Cybersegurança para servidores, estações de trabalho e demais sensores de rede com gerenciamento da superfície de risco e microsegmentação de aplicações com visibilidade de conexões e contenção da rede, para a infraestrutura da SEMIT, na modalidade de subscrição de licença, incluindo suporte técnico no regime 24x7 (vinte e quatro horas por dia, sete dias por semana) e garantia de atualização das versões pelo período de 24 meses, contemplando também, instalação, configuração e treinamento de acordo com as especificações técnicas mínimas e detalhamentos consignados neste Termo de Referência (TR) e seus anexos, com a conveniência e necessidade da Prefeitura Municipal de Salvador – PMS, conforme as especificações, quantitativas e qualitativas e todas as demais condições gerais discorridas neste Termo de Referência (TR).

2 JUSTIFICATIVA DA CONTRATAÇÃO

2.0 A Secretaria Municipal de Inovação e Tecnologia – SEMIT tem entre as suas competências, viabilizar o acesso seguro, controlado e ágil às informações, através da infraestrutura de Tecnologia da Informação e Comunicação – TIC para todos os órgãos e entidades da Prefeitura Municipal do Salvador – PMS.

2.1 **Lote Único**

2.2 Grupo 01 – Solução de Cybersegurança para Servidores, estações de trabalho com gerenciamento da superfície de risco:

2.3 A aquisição de soluções de Cybersegurança objetos desta licitação possui, como intuito, prevenir a contaminação por códigos maliciosos, suas variantes e demais ameaças cibernéticas, nos computadores dos Órgãos da Prefeitura Municipal do Salvador, mitigando o risco e preservando o sigilo, a integridade e a disponibilidade das informações.

2.4 O dinamismo no surgimento de novas tecnologias e a crescente demanda surgem as necessidades permanentes em manter-se alta disponibilidade, alto desempenho, segurança e controle para que todos os usuários, das redes dependentes direta ou indiretamente da Secretaria Municipal de Inovação e Tecnologia – SEMIT, possam exercer suas atividades de rotina, proporcionando melhor qualidade nas ações corporativas da PMS.

2.5 A expansão das ferramentas do fabricante TREND MICRO atualmente em uso na SEMIT com novas tecnologias do fabricante, visam a continuidade das adoções de providências necessárias para agilizar a tomada de decisões que exigem celeridade, otimizando as ações da máquina administrativa, reduzindo os riscos de indisponibilidade dos sistemas, reduzindo a probabilidade de êxito em ataques cibernéticos, proporcionando monitoração contínua e efetiva da infraestrutura e dos serviços de TIC, além de ampliar a proteção dos dados prevista no Marco Civil da Internet e na Lei Geral de Proteção de dados, LGPD.

2.6 A importância da integração entre essas ferramentas existentes e novas tecnologias a serem adquiridas deve ser garantida para preservar uma gerência global sobre as mesmas e a capacidade de correlacionar eventos detectados nos diversos sensores da solução. A contratação destas ferramentas justifica-se para garantir a segurança do ambiente

de TIC da SEMIT e das Unidades da Prefeitura Municipal do Salvador.

2.7 Grupo 2 – Solução de Cybersegurança para Microsegmentação de aplicações com visibilidade de conexões e contenção da rede

2.8 Implementação de mecanismos de isolamento granular de cargas de trabalho e seus fluxos de rede em função da obrigatoriedade dos processos individuais utilizados nos servidores e containers, com o objetivo de reduzir a superfície de ataque, garantir maior visibilidade e divisão da rede em segmentos menores, restringindo tráfego Leste-Oeste, fortalecer a contenção de ameaças por meio das políticas de segurança dinâmicas.

2.9 A utilização de solução de microsegmentação aumenta a proteção de rede e torna-se fundamental para garantir proteção de ambientes complexos e altamente distribuídos, como os encontrados nos sistemas governamentais, que venha garantir eficiência na detecção de ameaças e violações, reduzindo o tempo de resposta a incidentes.

2.10 Insights com busca capaz detectar plataformas e dispositivos de alto risco no ambiente.

2.11 Orquestração de políticas de segurança detalhadas para cada segmento da rede, baseado na visibilidade histórica dos fluxos de rede e da comunicação com processos existentes em função da ampla e granular proteção dos segmentos de rede que atuam de forma independente para garantia de segurança dos ambientes. As aplicações destas políticas garantem maior agilidade e flexibilidade na resposta de incidentes, permitindo de forma granular isolar rapidamente um segmento de rede inteiro, bem como isolar apenas o processo de comunicação, permitindo assim a continuidade de serviços ativos dentro do mesmo servidor infectado.

2.12 Prevenção de movimentação lateral com detecção de brechas através da microsegmentação, com visibilidade efetiva e monitoramento de comunicação para todas as cargas de trabalho.

2.13 Ampla cobertura de plataformas para tecnologias legadas e sistemas mais recentes.

2.14 A adoção de uma solução de Microsegmentação, Visibilidade e Contenção do Tráfego de Rede é particularmente relevante no contexto da SEMIT, para garantia da integridade dos dados sensíveis e continuidade dos serviços essenciais, com controle, proteção, e visibilidade das interações entre os sistemas do ambiente e para com o ambiente controlado pela aplicação, o que aprimora e otimiza a segurança em geral através do gerenciamento granular de redes distribuídas e complexas. Essa abordagem moderna de segurança fortalece o ecossistema digital, alinhando-se às demandas estratégicas de proteção de dados e garantindo uma infraestrutura mais resiliente, menos vulnerável a falhas, ataques internos e externos.

2.15 Pode-se elencar abaixo os pontos de destaque aos benefícios projetados:

2.16 Convergência tecnológica desejada e necessária à implementação de todos os eixos e estratégias da Administração Municipal.

2.17 Alinhamento estratégico de planejamento, orientados pela Secretaria Municipal de Inovação e Tecnologia – SEMIT;

2.18 Maior qualidade da dos serviços de TIC da PMS e da Secretaria Municipal de Inovação e Tecnologia – SEMIT;

2.19 Gerenciamento e segurança eficiente e proativo da rede e serviços de TIC da PMS e da Secretaria Municipal de Inovação e Tecnologia – SEMIT;

2.20 Monitoração contínua e efetiva da infraestrutura e dos serviços de TIC da PMS e

da Secretaria Municipal de Inovação e Tecnologia – SEMIT;

2.21 Aumento do grau de satisfação dos usuários com os serviços de TIC da PMS;

2.22 Ampliar a visibilidade e o controle do uso da Infraestrutura e dispositivos aderente ao Plano Estratégico orientada à Governa e Políticas de Acesso;

2.23 Ampliar proteção contra riscos iminentes de ciberataques associados às ameaças de Ransomware, tais como WannaCry e Petya;

2.24 Ampliar proteção contra risco potencial associado a conexões indevidas e maliciosas às aplicações;

2.25 Ampliar proteção contra risco potencial associado a Movimentação Lateral e conexões de rede;

2.26 Ampliar proteção contra risco latente nos sistemas operacionais legados;

2.27 A utilização do sistema de registro de preços justifica-se por tratar-se de objeto cuja contratação será de forma parcelada e sem garantia de saque total, em função das incertezas acerca do tempo e da efetivação da implantação devido à complexidade do ambiente operacional refletida na diversidade de versões dos sistemas existentes no parque tecnológico.

3 DESCRIÇÃO E QUANTITATIVOS DO OBJETO

3.0 A modalidade desta licitação será em Lote Único discriminados em dois grupos neste Termo de Referência;

3.1 A solução ofertada deverá existir como produto pronto antes do lançamento do edital, não sendo aceitos produtos em fase alfa, beta ou qualquer fase anterior à versão final e estável;

3.2 Segue detalhamento dos itens conforme tabela abaixo:

LOTE ÚNICO		
Grupo 1 – Solução de Cybersegurança para Servidores, Estações de Trabalho com Gerenciamento da Superfície de Risco		
Item	**Descrição**	**Qtd.**
1	Trend Micro Vision One Endpoint Security Pro, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	1.500
2	Trend Micro Email and Collaboration Security, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	34.000
3	Trend Micro Deep Discovery Inspector – 4Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	4
4	Trend Micro TippingPoint Threat Protection System (TPS) 5Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	4
5	Trend Micro TippingPoint Threat Protection System (TPS) 10Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	3
6	Trend Micro – Plataforma TrendAi Vision One por 24 (vinte e quatro) meses	500.000
7	Trend Micro Service One Complete (rede 4Gbps) por 24 (vinte e	4

	quatro) meses	
8	Trend Micro Service One Complete (endpoint) por 24 (vinte e quatro) meses	1.500
9	Network Packet Broker, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	2
10	Módulo mini-gbic SFP+ gigabit Ethernet Base-SR, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	40
11	Módulo mini-gbic SFP gigabit Ethernet 10GBASE-T, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	24
12	Funcionalidade de Descriptografia de Rede SSL/TLS em linha, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	2
13	Funcionalidade de Otimização de Cópia de Tráfego para Ferramentas, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	2
14	Gerência Centralizada - Network Packet Broker, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	1
15	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 1	1.500
16	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 2	34.000
17	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 3	4
18	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 4	4
19	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 5	3
20	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 9	2
21	Treinamento oficial	15
Grupo 2 – Solução de Cybersegurança para Microsegmentação de Aplicações com Visibilidade de Conexões e Contenção da Rede		
22	**Solução de microssegmentação, visibilidade e proteção de Rede, baseada em Software, para controle de movimentação lateral em ambiente corporativo de servidores**	1.500
23	**Solução de microssegmentação, visibilidade e proteção de Rede, baseada em Software, para controle de movimentação lateral em ambiente corporativos em Containers**	50
24	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 22	1.500
25	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 23	50
26	Treinamento oficial	15

4 ESPECIFICAÇÕES TÉCNICAS DETALHADAS – GRUPO 1

4.0 TREND VISION ONE ENDPOINT SECURITY PRO

4.1 Trend Vision One Endpoint Security Pro é sensor de segurança para servidores físicos, virtuais e em nuvem, projetada para proteger aplicações empresariais e dados contra violações e interrupções de negócios sem a necessidade de patching emergencial.

4.2 Componentes Principais:

4.3 Console de Segurança de carga de trabalho:

4.4 Console de Gerenciamento Centralizado com Interface web que os administradores usam para configurar políticas de segurança e implantar proteção nos componentes de aplicação.

4.5 Agente de Segurança é Instalado diretamente nos computadores, fornecendo controle de aplicação, anti-malware, serviço de reputação web, firewall, prevenção de intrusão, monitoramento de integridade e inspeção de logs.

4.6 Módulo Relay:

4.7 Distribuição de Atualizações: Agente habilitado para relay distribui atualizações de software e segurança em toda a rede de componentes de Endpoint Security Pro.

4.8 Notifier:

4.9 Comunicação de Status de Segurança: Aplicativo que comunica informações sobre o status de segurança e eventos no computador local, além de fornecer informações sobre atualizações de segurança distribuídas.

4.10 Virtual Patching:

4.11 Virtual Patching é uma tecnologia que fornece proteção contra vulnerabilidades sem a necessidade de aplicar patches físicos imediatamente. Isso é especialmente útil para proteger sistemas que não podem ser atualizados rapidamente devido a restrições operacionais ou compatibilidade.

4.12 Detalhe de Funcionamento:

4.13 Detecção de Vulnerabilidades;

4.14 Monitoramento Contínuo: O sistema monitora continuamente as vulnerabilidades conhecidas e desconhecidas em aplicações e sistemas.

4.15 Análise de Tráfego: Inspeciona o tráfego de rede para identificar tentativas de exploração de vulnerabilidades.

4.16 Aplicação de Proteção:

4.17 Utiliza filtros de proteção, conhecidos como Digital Vaccine, para bloquear tentativas de exploração antes que possam atingir o sistema.

4.18 Implementa regras de prevenção de intrusão para interceptar ataques em tempo real.

4.19 Atualizações e Manutenção:

4.20 Atualizações Automáticas: Recebe atualizações automáticas de novos filtros e regras de proteção para garantir que a segurança esteja sempre atualizada.

4.21 Gerenciamento Centralizado: Permite que administradores gerenciem e monitorem a aplicação de virtual patching a partir de um console centralizado.

4.22 Módulos de Proteção:

4.23 Anti-Malware: Protege workloads Windows e Linux contra malware, spyware e trojans. Utiliza a Trend Micro Smart Protection Network para identificar e remover malware

e bloquear domínios conhecidos como servidores de comando e controle.

4.24 Firewall: Controla o tráfego de entrada e saída e mantém logs de eventos de firewall para auditorias.

4.25 Web Reputation: Protege contra ataques que começam com visitas a URLs maliciosas, bloqueando o acesso a sites perigosos.

4.26 Device Control: Gerencia e controla o uso de dispositivos conectados ao sistema, como USBs e outros periféricos.

4.27 Activity Monitoring: Monitora atividades suspeitas e comportamentos anômalos no sistema.

4.28 Application Control: Permite que apenas aplicações autorizadas sejam executadas no sistema, prevenindo a execução de software não autorizado.

4.29 Intrusion Prevention: Protege contra tentativas de exploração de vulnerabilidades, interceptando ataques em tempo real.

4.30 Integrity Monitoring: Detecta e alerta sobre mudanças inesperadas em arquivos e configurações críticas.

4.31 Log Inspection: Analisa logs de eventos para identificar atividades suspeitas e violações de segurança.

4.32 Container Protection: Aplica módulos de proteção a containers, garantindo segurança em ambientes de conteinerização.

4.33 TREND MICRO EMAIL AND COLLABORATION SECURITY

4.34 Trend Micro Vision One Email Collaboration Security é sensor de segurança projetada para proteger contas de e-mail e aplicativos de colaboração em nuvem contra ameaças sofisticadas, como phishing, malware, ransomware e ataques direcionados.

4.35 Componentes Principais:

4.36 Console de Gerenciamento Centralizado;

4.37 Visibilidade Unificada: Interface web que permite aos administradores gerenciar e monitorar a segurança de todos os endpoints e workloads em um ambiente multi-nuvem.

4.38 Automação de Proteção: Implementa políticas de segurança contextualmente conscientes e controle de acesso baseado em funções.

4.39 Módulos de Proteção:

4.40 Anti-Malware - Proteção Contra Malware - Protege contas de e-mail e aplicativos de colaboração contra malware, spyware e trojans. Utiliza a Trend Micro Smart Protection Network para identificar e remover malware e bloquear domínios conhecidos como servidores de comando e controle.

4.41 Proteção Contra Phishing - Detecção de Phishing: Identifica e bloqueia tentativas de phishing, protegendo os usuários contra roubo de credenciais e informações sensíveis.

4.42 Proteção Contra Ransomware - Detecção de Ransomware: Detecta e bloqueia ataques de ransomware, prevenindo a criptografia de dados e garantindo a continuidade dos negócios.

4.43 Prevenção de Fraude - Detecção de Fraude: Monitora e bloqueia tentativas de fraude, protegendo contra ataques que visam enganar os usuários para obter informações financeiras.

4.44 Proteção Contra Ataques Direcionados - Detecção de Ataques Direcionados: Utiliza análise avançada para identificar e bloquear ataques direcionados que visam comprometer contas de e-mail e aplicativos de colaboração.

4.45 Monitoramento de Atividades - Monitoramento de Atividades: Monitora atividades suspeitas e comportamentos anômalos em contas de e-mail e aplicativos de colaboração.

4.46 Análise de Sandbox - Análise de Sandbox: Utiliza sandboxing para analisar anexos e links suspeitos em um ambiente isolado, identificando e bloqueando ameaças antes que possam causar danos.

4.47 TREND MICRO DEEP DISCOVERY INSPECTOR – 4GBPS, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.48 Trend Micro Deep Discovery Inspector é um sensor de detecção e resposta a ameaças (NDR) que permite a detecção em toda a rede de ataques direcionados, ameaças avançadas e ransomware sem interromper as operações.

4.49 Componentes Principais:

4.50 Appliance de Rede com monitoramento 360 Graus. O appliance, que pode ser físico ou virtual, monitora toda a rede, proporcionando visibilidade completa de taques direcionados, ameaças avançadas e ransomware.

4.51 Motores de Detecção Especializados com Análise de Sandbox Personalizada, utiliza motores de detecção especializados e análise de sandbox personalizada para identificar malware avançado, ransomware, exploits de zero-day, comunicações de comando e controle (C&C) e atividades evasivas de atacantes.

4.52 Compartilhamento de Inteligência de Ameaças, utiliza padrões como STIX, TAXII e YARA para compartilhar inteligência de ameaças avançadas com soluções de segurança da Trend Micro e de terceiros.

4.53 Funcionalidades Principais:

4.54 Detecção de Tráfego de Rede:

4.55 Monitoramento de todo o tráfego de rede, incluindo tráfego físico, virtual e mais de 100 protocolos de rede.

4.56 Identifica movimentos laterais, atividades de C&C e outros comportamentos de atacantes em todas as fases do ciclo de ataque.

4.57 Análise Gráfica de Ataques:

4.58 Fornece uma análise gráfica detalhada dos ataques, permitindo que as equipes de segurança visualizem e respondam a ameaças em tempo real.

4.59 Automação de Tarefas Manuais:

4.60 Automatiza tarefas manuais, como a análise de logs e a resposta a incidentes, aumentando a eficiência operacional.

4.61 Integração com IA:

4.62 Detecção Aprimorada utilizando aprendizado de máquina e IA para melhorar a detecção de ameaças avançadas e ransomware.

4.63 Benefícios:

4.64 Proporciona visibilidade completa de todas as atividades de rede, permitindo uma resposta rápida e eficaz às ameaças.

4.65 Melhora a taxa de detecção de ameaças avançadas e ransomware projetados para evadir defesas de segurança padrão.

4.66 Oferece opções de implantação flexíveis, permitindo que as organizações escolham entre appliances físicos ou virtuais.

4.67 TREND MICRO TIPPINGPOINT THREAT PROTECTION SYSTEM (TPS) 5GBPS,

INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.68 Trend Micro TippingPoint é um sensor de segurança de rede de alto desempenho, projetada para fornecer proteção abrangente contra ameaças conhecidas e desconhecidas com alta precisão.

4.69 Componentes Principais:

4.70 Appliance de Rede:

4.71 Monitoramento 360 Graus - Os appliances monitoram toda a rede, proporcionando visibilidade completa de ataques direcionados, ameaças avançadas e ransomware.

4.72 Motores de Detecção Especializados:

4.73 Análise de Pacotes Profunda - Utiliza inspeção profunda de pacotes (DPI), reputação de ameaças, reputação de URLs e análise avançada de malware para detectar e prevenir ataques na rede.

4.74 Compartilhamento de Inteligência de Ameaças:

4.75 Padrões de Compartilhamento: Utiliza padrões como STIX, TAXII e YARA para compartilhar inteligência de ameaças avançadas com soluções de segurança da Trend Micro e de terceiros.

4.76 Informações de Hardware

4.77 Portas: Duas portas QSFP+ fixas para propósito especial (SP), uma porta de console RJ-45, uma porta de gerenciamento 1 GbE copper.

4.78 Slots: Quatro slots de I/O.

4.79 Fonte de Alimentação: Uma fonte de alimentação AC substituível de 250W.

4.80 Modulo de Bypass

4.81 Funcionalidades Principais:

4.82 Inspecionar throughput de 05 Gbps;

4.83 Latência igual ou inferior a 60 Microsegundos;

4.84 Suporta 400.000 novas conexões por segundo;

4.85 Suporta 30 milhões de sessões concorrentes;

4.86 Suporta 3000 novas conexões SSL por segundo;

4.87 Suporta inspeção de tráfego SSL de até 3,5 Gbps;

4.88 Fornece funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);

4.89 Detecção de Tráfego de Rede:

4.90 Monitoramento de Tráfego: Monitora todo o tráfego de rede, incluindo tráfego físico, virtual e mais de 100 protocolos de rede.

4.91 Detecção de Movimento Lateral: Identifica movimentos laterais, atividades de C&C e outros comportamentos de atacantes em todas as fases do ciclo de ataque.

4.92 Análise Gráfica de Ataques:

4.93 Visualização de Ataques: Fornece uma análise gráfica detalhada dos ataques, permitindo que as equipes de segurança visualizem e respondam a ameaças em tempo real.

4.94 Automação de Tarefas Manuais:

4.95 Automação: Automatiza tarefas manuais, como a análise de logs e a resposta a incidentes, aumentando a eficiência operacional.

4.96 Integração com IA:

4.97 Detecção Aprimorada: Utiliza aprendizado de máquina e IA para melhorar a detecção de ameaças avançadas e ransomware.

4.98 Benefícios:

4.99 Visibilidade Completa

4.100 Proporciona visibilidade completa de todas as atividades de rede, permitindo uma resposta rápida e eficaz às ameaças.

4.101 Detecção Aprimorada:

4.102 Melhora a taxa de detecção de ameaças avançadas e ransomware projetados para evadir defesas de segurança padrão.

4.103 Flexibilidade de Implantação:

4.104 Oferece opções de implantação flexíveis, permitindo que as organizações escolham entre appliances físicos ou virtuais.

4.105 TREND MICRO TIPPINGPOINT THREAT PROTECTION SYSTEM (TPS) 10GBPS, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.106 Trend Micro TippingPoint é um sensor de segurança de rede de alto desempenho, projetada para fornecer proteção abrangente contra ameaças conhecidas e desconhecidas com alta precisão.

4.107 Componentes Principais:

4.108 Appliance de Rede:

4.109 Monitoramento 360 Graus - Os appliances monitoram toda a rede, proporcionando visibilidade completa de ataques direcionados, ameaças avançadas e ransomware.

4.110 Motores de Detecção Especializados:

4.111 Análise de Pacotes Profunda - Utiliza inspeção profunda de pacotes (DPI), reputação de ameaças, reputação de URLs e análise avançada de malware para detectar e prevenir ataques na rede.

4.112 Compartilhamento de Inteligência de Ameaças:

4.113 Padrões de Compartilhamento: Utiliza padrões como STIX, TAXII e YARA para compartilhar inteligência de ameaças avançadas com soluções de segurança da Trend Micro e de terceiros.

4.114 Informações de Hardware

4.115 Portas: Duas portas QSFP+ fixas para propósito especial (SP), uma porta de console RJ-45, uma porta de gerenciamento 1 GbE copper.

4.116 Slots: Quatro slots de I/O.

4.117 Fonte de Alimentação: Uma fonte de alimentação AC substituível de 250W.

4.118 Modulo de Bypass

4.119 Funcionalidades Principais:

4.120 Inspecionar throughput de 10 Gbps;

4.121 Latência igual ou inferior a 40 Microsegundos;

4.122 Suporta 650.000 novas conexões por segundo;

4.123 Suporta 120 milhões de sessões concorrentes;

4.124 Suporta 5700 novas conexões SSL por segundo;

4.125 Suporta inspeção de tráfego SSL de até 8 Gbps;

4.126 Fornece funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);

4.127 Detecção de Tráfego de Rede:

4.128 Monitoramento de Tráfego: Monitora todo o tráfego de rede, incluindo tráfego físico, virtual e mais de 100 protocolos de rede.

4.129 Detecção de Movimento Lateral: Identifica movimentos laterais, atividades de C&C e outros comportamentos de atacantes em todas as fases do ciclo de ataque.

4.130 Análise Gráfica de Ataques:

4.131 Visualização de Ataques: Fornece uma análise gráfica detalhada dos ataques, permitindo que as equipes de segurança visualizem e respondam a ameaças em tempo real.

4.132 Automação de Tarefas Manuais:

4.133 Automação: Automatiza tarefas manuais, como a análise de logs e a resposta a incidentes, aumentando a eficiência operacional.

4.134 Integração com IA:

4.135 Detecção Aprimorada: Utiliza aprendizado de máquina e IA para melhorar a detecção de ameaças avançadas e ransomware.

4.136 Benefícios:

4.137 Visibilidade Completa

4.138 Proporciona visibilidade completa de todas as atividades de rede, permitindo uma resposta rápida e eficaz às ameaças.

4.139 Detecção Aprimorada:

4.140 Melhora a taxa de detecção de ameaças avançadas e ransomware projetados para evadir defesas de segurança padrão.

4.141 Flexibilidade de Implantação:

4.142 Oferece opções de implantação flexíveis, permitindo que as organizações escolham entre appliances físicos ou virtuais.

4.143 TREND MICRO PLATAFORMA TRENDAI VISION ONE – POR 24 (VINTE E QUATRO) MESES.

4.144 Deve possuir plataforma WEB de segurança cibernética unificada que ofereça abordagem integrada para a gestão do risco de superfície de ataque e detecção e resposta estendida (XDR).

4.145 Deve permitir a detecção e resposta além do endpoint, oferecendo uma visibilidade mais ampla e análises de segurança especializadas, o que leva a mais detecções e uma resposta mais rápida;

4.146 Deve realizar o gerenciamento de risco da superfície de ataque;

4.147 Deve Combinar gerenciamento de superfície de ataque e XDR em um único console para gerenciar o risco cibernético de toda a organização de maneira centralizada;

4.148 Deve fornecer suporte a ambientes de TI híbridos diversos,

4.149 Deve permitir automatizar e orquestra fluxos de trabalho e entregar serviços de

segurança cibernética especializados,

4.150 Deve permitir centralizar as operações de segurança para uma única plataforma e fornecer uma métrica que quantifique o valor de risco da estrutura completa, incluindo ambientes híbridos com serviços em nuvem.

4.151 Deve utilizar inteligência artificial

4.152 Deve permitir a integração nativa via API com outros fabricantes de solução de segurança para a composição de uma visão de segurança centralizada.

4.153 Deve ser capaz de enviar e receber dados de telemetria oriundos das integrações nativas via API.

4.154 TREND MICRO SERVICE ONE COMPLETE (REDE 4Gbps), POR 24 (VINTE E QUATRO) MESES

4.155 Permite que a CONTRATANTE se comunique diretamente com o fabricante no regime 24 horas por dia, 7 dias por semana para abertura de casos de suporte relativos ao funcionamento das soluções no escopo, bem como a ameaças no ambiente ou dúvidas gerais sobre segurança da informação;

4.156 Fornece acesso a um gestor de serviços para comunicações gerais acerca do ambiente e das entregas contratadas, agindo como um ponto único de contato;

4.157 O gestor de serviço deverá entregar relatórios sobre o desempenho e entregas de forma periódica durante o contrato;

4.158 Possibilita acesso a aconselhamento sobre processos de melhoria, atualização ou migração das soluções para o gestor de serviços do fabricante;

4.159 Permite interação direta entre o fabricante e a CONTRATANTE;

4.160 Permite criação de relatórios dos incidentes analisados e reportados;

4.161 Provê monitoramento dos alertas gerados pela solução de gestão de detecção e resposta estendida 24 horas por dia e 7 dias por semana em função do Troughput capturado pelos sensores de rede da solução;

4.162 Cada unidade deste item corresponde ao monitoramento mínimo de 4 Gbps de troughput para os sensores de rede respectivos da solução em funcionamento;

4.163 A soma das unidades deste item é acumulativa, podendo habilitar o monitoramento em função do troughput total dos sensores de rede da solução, caso ultrapasse o mínimo de 05Gbps;

4.164 Os alertas gerados deverão ser analisados e categorizados segundo criticidade Alta, Média e Baixa;

4.165 O fabricante deverá analisar os logs gerados pelos sensores do XDR e deverá alertar em casos de possíveis indícios de fases iniciais ou em curso de ataques cibernéticos;

4.166 O fabricante deverá aplicar ao menos duas vezes análise de configurações detalhadas das soluções a fim de determinar a saúde das ferramentas;

4.167 Ao final de cada validação de saúde das soluções o fabricante deverá apresentar um relatório detalhado;

4.168 O fabricante deverá disponibilizar ao menos 25hrs por ano de serviços especializados de análise profundo de incidentes de segurança e respostas a incidente;

4.169 Ao final das atividades de incidente e resposta o fabricante deverá apresentar relatório conclusivo sobre as atividades realizadas;

4.170 A plataforma de investigação do serviço deve utilizar regras inteligentes com Machine Learning e Inteligência Artificial, em conjunto com a inteligência de ameaças do

fabricante.

4.171 TREND MICRO SERVICE ONE COMPLETE (ENDPOINT), POR 24 (VINTE E QUATRO) MESES

4.172 Permite que a CONTRATANTE se comunique diretamente com o fabricante no regime 24 horas por dia, 7 dias por semana para abertura de casos de suporte relativos ao funcionamento das soluções no escopo, bem como a ameaças no ambiente ou dúvidas gerais sobre segurança da informação;

4.173 Fornece acesso a um gestor de serviços para comunicações gerais acerca do ambiente e das entregas contratadas, agindo como um ponto único de contato;

4.174 O gestor de serviço deverá entregar relatórios sobre o desempenho e entregas de forma periódica durante o contrato;

4.175 Possibilita acesso a aconselhamento sobre processos de melhoria, atualização ou migração das soluções para o gestor de serviços do fabricante;

4.176 Permite interação direta entre o fabricante e a CONTRATANTE;

4.177 Permite criação de relatórios dos incidentes analisados e reportados;

4.178 Provê monitoramento dos alertas gerados pela solução de gestão de detecção e resposta estendida 24 horas por dia e 7 dias por semana em função da telemetria capturada pelos sensores de endpoint da solução;

4.179 Cada unidade deste item correnponde ao monitoramento de um endpoint;

4.180 Os alertas gerados deverão ser analisados e categorizados segundo criticidade Alta, Média e Baixa;

4.181 O fabricante deverá analisar os logs gerados pelos sensores do XDR e deverá alertar em casos de possíveis indícios de fases iniciais ou em curso de ataques cibernéticos;

4.182 O fabricante deverá aplicar ao menos duas vezes análise de configurações detalhadas das soluções a fim de determinar a saúde das ferramentas;

4.183 Ao final de cada validação de saúde das soluções o fabricante deverá apresentar um relatório detalhado;

4.184 O fabricante deverá disponibilizar ao menos 25hrs por ano de serviços especializados de análise profundo de incidentes de segurança e respostas a incidente;

4.185 Ao final das atividades de incidente e resposta o fabricante deverá apresentar relatório conclusivo sobre as atividades realizadas;

4.186 A plataforma de investigação do serviço deve utilizar regras inteligentes com Machine Learning e Inteligência Artificial, em conjunto com a inteligência de ameaças do fabricante.

4.187 NETWORK PACKET BROKER, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.188 CARACTERÍSTICAS TÉCNICAS GERAIS

4.189 O equipamento deve ser baseado em Appliance Box suportando montagem em rack (bastidor) de 19” (dezenove polegadas), com utilização de no máximo 1-RU (uma unidade de bastidor) de altura, com fornecimento dos respectivos conjuntos de fixação.

4.190 Os equipamentos ofertados deverão possuir funcionalidades e hardware específicos para este propósito de agregação, regeneração, filtragem e modificação/transformação do tráfego, não sendo aceita soluções similares, como: Switches, Roteadores, Firewalls, Balanceadores, Servidores, soluções Híbridas e etc.

4.191 A solução deverá ser composta por único fabricante, incluindo os itens de Agregador, módulos e GBICs, com vista a não desperdício de recursos técnicos e facilidade de integração.

4.192 Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de "Rede", "Rede Inline", "Ferramenta" e portas de "Ferramenta Inline".

4.193 Entende-se por portas de Rede, todas as portas que serão responsáveis por receber a cópia do tráfego através dos TAPs/SPANs.

4.194 Entende-se por portas de Ferramenta, todas as portas que serão responsáveis por encaminhar o tráfego, seja ele já filtrado e/ou modificado, para as ferramentas que serão conectadas a solução de NPB.

4.195 Entende-se por portas de Rede Inline, todas as portas que serão responsáveis por se conectar de forma Inline a rede de produção.

4.196 Entende-se por portas de Ferramenta Inline, todas as portas que serão responsáveis por encaminhar o tráfego de produção, selecionado através dos filtros ou não, para as ferramentas Inline que serão conectadas a solução de NPB.

4.197 A solução deverá suportar interfaces de 1, 10 e 40 Gbps através da adição ou substituição módulos/licenças, sem causar impacto no desempenho dos equipamentos ofertados.

4.198 O equipamento deverá possuir a capacidade de processamento de, no mínimo, 600 (seiscentos) Gbps de tráfego agregado para aplicação dos filtros (regras) descritos nesta especificação.

4.199 O equipamento deve estar em conformidade com o padrão RoHS.

4.200 Deverá possuir módulos de ventilação hot swappable;

4.201 Possuir ventilação "front-to-back", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento.

4.202 Deverá possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable.

4.203 Deverá possuir fonte de alimentação AC redundante interna, hot-swappable.

4.204 Deverá suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento

4.205 São apresentadas, a seguir, as especificações técnicas mínimas a serem ofertadas referentes ao objeto. Os termos "possuir", "permite/permitir", "implementar" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

4.206 A solução é definida como um Network Packet Broker, ou seja, realiza características de um broker a nível de pacotes de rede. Uma solução específica caracterizada como SSL Decryption ou com funcionalidade de SSL Inspection realiza apenas uma das múltiplas funções de um Network Packet Broker. Desta forma, não serão aceitas soluções como Firewalls UTM, Next-Generation Firewall (NGFW), Load Balancers com funcionalidade de SSL Offloading, e tais atestados não serão considerados como válidos.

4.207 GERENCIAMENTO DO NETWORK PACKET BROKER:

4.208 Deverá permitir configuração customizada baseadas nos perfis de acesso (RBAC - Role Base Access Control).

4.209 Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3,

incluindo a geração de traps.

4.210 Deverá possuir suporte a MIB II.

4.211 Deverá implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

4.212 Deverá suportar SNMP trap sobre IPv6.

4.213 Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface de gerenciamento.

4.214 Deverá permitir a gravação de log externo (syslog).

4.215 Deverá permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação

4.216 Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos.

4.217 Deve suportar configuração total da solução através de console local RS-232 ou RJ-45.

4.218 Deve possuir gerenciamento através de interface Web (HTTPS) ou CLI.

4.219 Deverá implementar o protocolo NTP (Network Time Protocol).

4.220 Deverá implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP.

4.221 Deve suportar IPv6 para TACACS+.

4.222 Deverá implementar o protocolo SSHv2 para acesso à interface de linha de comando

4.223 Deverá proteger a interface de comando do equipamento através de senha.

4.224 **FILTROS (REGRAS):**

4.225 A solução deverá implementar as seguintes configurações para agregação e encaminhamento de pacotes das portas de Rede para as portas de Ferramentas, tanto para os fluxos out-of-Band (Cópia de Tráfego) quanto para Inline, respectivamente:

4.226 Uma para uma;

4.227 Uma para Várias - Com suporte a balanceamento;

4.228 Várias para uma;

4.229 Várias para Várias - Com suporte a balanceamento;

4.230 Deverá permitir criar filtros (regras) baseados em, no mínimo, os seguintes campos:

4.231 Endereços MAC de origem e destino;

4.232 Endereço IPv4 de origem/destino;

4.233 Portas TCP e UDP de origem e destino;

4.234 VLAN ID;

4.235 Ethertype;

4.236 IPFrag;

4.237 TTL;

4.238 TOS;

4.239 Protocol;

4.240 TCP Control Mask/Bits;

4.241 DSCP;

4.242 Versão do Protocolo IPv4 e IPv6;

4.243 Endereço IPv6 de origem/destino;

4.244 A solução deverá suportar, no mínimo, 16000 (dezesseis mil) filtros (regras).

4.245 Deverá permitir a inserção e remoção de novos filtros (regras) sem a necessidade de reiniciar o(s) equipamento(s), ou seja, a aplicação destes filtros (regras) deverá acontecer em tempo real.

4.246 Deve suportar overlapping de filtros (regras), ou seja, utilização conjunta de filtros de entrada (ingress) e filtros de saída (egress).

4.247 A solução deverá suportar funcionalidade Mesh/Cluster.

4.248 O Mesh/Cluster deverá permitir a configuração e gerenciamento de 2 (dois) ou mais agregadores como um único equipamento lógico. Não serão aceitas soluções em cascata para o atendimento desta funcionalidade.

4.249 A solução deverá suportar, no mínimo, 30 agregadores em modo Mesh/Cluster.

4.250 O Mesh/Cluster deverá permitir a configuração de todos os Agregadores a partir de uma única interface WEB (HTTPS) e CLI.

4.251 A funcionalidade de Mesh/Cluster deverá suportar a criação de 1 (um) ou mais filtros (regras) que se utilizem de portas de Rede em um equipamento físico e direcionem este tráfego para portas de Ferramenta localizadas em outro equipamento físico, independentemente da quantidade de equipamentos entre estes equipamentos. Não serão aceitas soluções em cascata para o atendimento deste item.

4.252 A funcionalidade de Mesh/Cluster deve suportar arquitetura conhecida como Spine/Leaf, permitindo balanceamento do tráfego entre os Leafs e os Spines e também adicionando redundância a solução em caso de falha de um dos equipamentos.

4.253 Deve suportar o conceito de FABRIC que permite a criação de filtros que se estendem por múltiplos agregadores ou mesh/clusters de agregadores.

4.254 Deve permitir a configuração de circuitos entre mesh/clusters de agregadores, permitindo que o tráfego recebido em um cluster seja entregue para uma ferramenta em outro cluster.

4.255 FUNCIONALIDADES INLINE

4.256 O equipamento deve suportar instalação sem necessidade de reconfiguração de roteadores e switches, quando utilizado no modo de operação Inline.

4.257 O equipamento deve suportar, de forma simultânea e em interfaces distintas, os modos:

4.258 TAP/SPAN (Cópia de Tráfego);

4.259 Inline (Tráfego de Produção);

4.260 A solução deverá ser capaz de configurar a sequência das ferramentas Inline (Serial), quando possuir 2 (duas) ou mais ferramentas, pela qual os pacotes deverão ser encaminhados sequencialmente quando o agregador funcionar de forma Inline.

4.261 A solução deverá ser capaz de configurar um grupo de ferramentas Inline (Paralelo), quando possuir 2 (duas) ou mais ferramentas, pela qual os pacotes deverão ser balanceados entre as ferramentas quando o agregador funcionar de forma Inline.

4.262 A solução deverá permitir a configuração conjunta das funcionalidades Serial e Paralelo, permitindo criar uma sequência serial de ferramentas que estão em Paralelo.

4.263 A solução deverá permitir que ferramentas inline em modo standalone, serial e Paralelo, possam ter a flexibilidade de receber somente o tráfego de interesse, sem impacto entre elas e sem a necessidade de solução de contorno físico. Por exemplo, a ferramenta 1 precisa receber todo o tráfego e a ferramenta 2 necessita receber apenas tráfego WEB, nesse tipo de cenário as ferramentas devem receber o tráfego desejado sem necessidade de arranjos físicos e sem impactar o tráfego da outra.

4.264 Suportar funcionalidade conhecida como Fail-Safe através do uso de bypass, que mesmo em caso de perda de energia, os links interceptados da rede continuem ativos, não gerando indisponibilidade de rede.

4.265 A solução deve suportar Heartbeat para monitoramento da saúde das ferramentas, quando utilizadas de forma Inline, permitindo detectar e remover somente a ferramenta que apresentar falha, sem causar impacto no fluxo de dados das outras ferramentas e no tráfego de rede.

4.266 A solução deve suportar Heartbeat Negativo, que permite utilizar um pacote específico para a geração do tráfego de checagem, no entanto, este pacote deve ser bloqueado pela ferramenta inline, não retornando novamente para a solução de NPB. Caso este pacote retorne a ferramenta inline será considerada com falha e deverá ser removida sem impacto na rede e nos fluxos de dados.

4.267 A solução, quando utilizada em modo Inline, deve permitir remover uma ou mais ferramentas da sequência do tráfego sem causar impacto no tráfego da rede. Esta funcionalidade tem como principal objetivo remover ferramentas para atualização e para fins de troubleshooting, sem causar interrupção de rede.

4.268 A solução deve permitir a alteração do modo de operação sem causar interrupção de rede da ferramenta inline para “simulação inline” sem causar interrupção de rede, de modo que a ferramenta entenda que está inline mas está recebendo apenas uma cópia dos dados que foram encaminhados para rede.

4.269 INTERFACES

4.270 A solução deverá implementar, no mínimo, 4 (oito) interfaces 1000BASE-T.

4.271 A solução deverá implementar, no mínimo, 24 (vinte e quatro) interfaces 1/10G SFP/SFP+.

4.272 O equipamento, independentemente do número de interfaces, deve ser fornecido com todas as suas portas licenciadas para funcionamento;

4.273 A garantia e todas as licenças devem ser fornecidas com vigência e suporte por 24 (vinte e quatro) meses;

4.274 FUNCIONALIDADES AVANÇADAS

4.275 Deve suportar funcionalidade Tunnel, que permite encapsulamento e desencapsulamento de tráfego entre 2 (dois) equipamentos através de redes L3 (roteadas).

4.276 A funcionalidade de Tunnel deve suportar o encapsulamento e o desencapsulamento utilizando protocolo L2GRE ou similar, permitindo transportar o tráfego encapsulado através de diferentes redes L3.

4.277 Deve suportar o balanceamento de carga dos pacotes de encapsulamento IPv6 L2GRE.

4.278 A solução deverá suportar balanceamento entre diferentes túneis, permitindo utilizar duas ou mais ferramentas da mesma solução como destino para todo o tráfego encapsulado.

4.279 Deve suportar a funcionalidade Packet Trimming (Corte do Pacote), otimizando o

tráfego que será encaminhado para as ferramentas reduzindo o tamanho do pacote.

4.280 A funcionalidade de Packet Trimming deve ser configurável para cortar o pacote das seguintes formas:

4.281 Corte, ou seja, definir se todos os pacotes de uma sessão, a partir de um número especificado, serão cortados;

4.282 Drop, ou seja, definir se todos os pacotes de uma sessão, a partir de um número especificado, serão eliminados;

4.283 Deve suportar a funcionalidade Packet Trimming (Corte do Pacote), otimizando o tráfego que será encaminhado para as ferramentas reduzindo o tamanho do pacote.

4.284 A funcionalidade de Packet Trimming deve ser configurável para cortar o pacote das seguintes formas:

4.285 Dinâmico, ou seja, a partir de um campo específico do cabeçalho ethernet definido pelo usuário;

4.286 Estático, ou seja, a partir de um offset específico definido pelo usuário;

4.287 Deve suportar terminação ERSPAN, permitindo terminar um tráfego espelhado de equipamentos que suportam ERSPAN.

4.288 Deve suportar terminação ERSPAN para as versões II e III.

4.289 Deve suportar a funcionalidade Masking (Alteração de dados), que é capaz de modificar determinadas informações contidas no tráfego de rede antes de redirecioná-lo para as Ferramentas, para atendimento de normas PCI quando necessário.

4.290 A funcionalidade Masking deverá ser capaz de trocar uma determinada informação como o CPF do usuário por outros caracteres (XXX.XXX.XXX-XX, por exemplo), de modo que essa informação específica seja protegida antes de ser enviada para as soluções.

4.291 Deve suportar a funcionalidade Protocol Stripping (Remoção de Cabeçalho), permitindo identificar e remover TAGs de VLANs e cabeçalhos específicos dos pacotes de rede.

4.292 A funcionalidade de Protocol Stripping deve suportar a remoção de pelo menos os seguintes cabeçalhos:

4.293 ERSPAN

4.294 VLAN;

4.295 MPLS;

4.296 VNTag;

4.297 VxLAN;

4.298 Fabric Path;

4.299 GRE;

4.300 ISL;

4.301 QinQ;

4.302 GTP;

4.303 A funcionalidade de Protocol Stripping também deverá suportar a remoção de cabeçalhos que não estejam pré-definidos, permitindo assim a customização de um offset e quantidade de bytes deverão ser removidos, permitindo assim a remoção de cabeçalhos não padronizados.

4.304 Deve suportar a funcionalidade Packet De-Duplication (De-duplicação de Pacotes),

enviando somente uma única cópia do pacote para as Ferramentas.

4.305 Deve suportar, no mínimo, processamento de 20 (vinte) Gbps para funcionalidade de Deduplicação de pacotes.

4.306 A funcionalidade de Packet De-Duplication deve suportar de-duplicação de pacotes IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o Payload e os cabeçalhos ethernet.

4.307 A funcionalidade Packet De-Duplication deve detectar pacotes duplicados recebidos em diferentes portas ou módulos do(s) equipamento(s), inclusive se utilizado em modo Mesh/Cluster, detectando pacotes duplicados entre diferentes portas, módulos e equipamentos.

4.308 A funcionalidade Packet De-Duplication deve permitir habilitar ou desabilitar a inspeção de, no mínimo, os seguintes campos para avaliar se é um pacote duplicado ou não:

4.309 IPv4 ToS;

4.310 IPv6 TC;

4.311 Número da Sequência TCP;

4.312 VLAN ID;

4.313 Deve suportar a funcionalidade de geração de metadados como NetFlow, IPFIX e CEF.

4.314 Deve suportar geração de NetFlow nas versões v5 e v9 e IPFIX.

4.315 Deve suportar a funcionalidade DPA (Deep Packet Analysis), que permita criar filtros (regras) que identifiquem qualquer informação dentro do pacote, desde o cabeçalho até o Payload.

4.316 A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando linguagem de programação Perl ou RegEx.

4.317 A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando uma string.

4.318 A funcionalidade DPA deve permitir a criação de filtros (regras) que façam "match" nos campos ethernet mesmo quando a informação estiver encapsulada por outros protocolos, como FCoE.

4.319 Deve suportar funcionalidade de Application Aware (App-Aware), que permite compreender uma sessão completa de um fluxo de dados e encaminhar/bloquear todos os pacotes subsequentes desta sessão para as Ferramentas.

4.320 A funcionalidade App-Aware deve suportar a utilização de buffer da sessão, permitindo armazenar, no mínimo, os 20 pacotes iniciais da sessão, para que nos casos onde o padrão da sessão for detectado após o handshake da sessão, todos os pacotes anteriores também sejam encaminhados para as Ferramentas.

4.321 Deve suportar a filtragem de tráfego com base na visibilidade da camada de aplicação, permitindo a identificação bidirecional do tráfego na camada 7 do modelo OSI através de funcionalidade de DPI (Deep Packet Inspection).

4.322 Deve suportar a identificação de, no mínimo, 3500 aplicações agrupadas por famílias ou grupos de aplicações tais como YouTube, Whatsapp e Gmail.

4.323 Deve suportar a definição de assinaturas para aplicações customizadas, incluindo protocolos e extensões proprietárias.

4.324 Após a identificação do tráfego com base na aplicação, a solução deve suportar a criação de filtros (regras) de encaminhamento e replicação de tráfego.

4.325 Deve suportar a funcionalidade SSL Decryption através de função Man-In-The-Middle e também somente cópia do tráfego.

4.326 MÓDULO MINI-GBIC SFP+ GIGABIT ETHERNET BASE-SR, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.327 Suportar o uso de fibra multimodo para distâncias de até 300 m (trezentos metros), conforme o padrão IEEE 10G Base-SR.

4.328 Possuir conector do tipo LC.

4.329 Permitir a inserção ou a remoção deste conector sem influenciar o funcionamento do equipamento ou módulo (Hot Swappable).

4.330 Deverá ser do mesmo fabricante dos demais itens.

4.331 A garantia deve ser fornecida com vigência e suporte por 24 (vinte e quatro) meses;

4.332 MÓDULO MINI-GBIC SFP GIGABIT ETHERNET 10GBASE-T, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.333 Suportar o uso de cabos UTP CAT 6 ou superior.

4.334 Possuir conector do tipo RJ-45.

4.335 Permitir a inserção ou a remoção deste conector sem influenciar o funcionamento do equipamento ou módulo (Hot Swappable).

4.336 Deverá ser do mesmo fabricante dos demais itens.

4.337 A garantia deve ser fornecida com vigência e suporte por 24 (vinte e quatro) meses;

4.338 FUNCIONALIDADE DE DESCRIPTOGRAFIA DE REDE SSL/TLS EM LINHA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.339 Deve ser compatível com o Network Packet Broker desse Termo de Referência.

4.340 Deve implementar a funcionalidade SSL Decryption através de função Man-In-The-Middle, através da instalação de módulos e licenças adicionais.

4.341 Os equipamentos, módulos, software e licenças utilizados para essa funcionalidade devem ser todos do mesmo fabricante do Network Packet Broker, facilitando assim a gerência e integração das soluções.

4.342 O equipamento deve implementar um throughput exclusivo de tráfego criptografado de, no mínimo, 4 (quatro) Gbps.

4.343 A descriptografia deve ser baseada no handshake SSL/TLS e não através de portas pré-definidas.

4.344 O equipamento deve permitir importação de no mínimo 1.000 (hum mil) certificados em formato PKCS #12 ou PEM.

4.345 Suportar, no mínimo, 8 mil novas conexões SSL por segundo, utilizando cifra 'TLS_RSA_WITH_AES_256_GCM_SHA384' e criptografia RSA de 2048 bits;

4.346 Suportar no mínimo 100 mil conexões SSL simultâneas utilizando criptografia de 2048 bits;

4.347 O equipamento deve suportar, no mínimo, os seguintes algoritmos de troca de chaves com autenticação:

4.348 RSA;

4.349 DHE_RSA;

4.350 ECDHE_RSA;

4.351 ECDHE_ECDSA;

4.352 O equipamento deve suportar, no mínimo, os seguintes métodos de autenticação de mensagens:

4.353 SHA;

4.354 SHA256;

4.355 SHA384;

4.356 POLY1305;

4.357 Deverá implementar Host Categorization, permitindo selecionar tráfegos que não serão descriptografados, como dados financeiros por exemplo.

4.358 A funcionalidade SSL Decryption deve suportar, no mínimo, os seguintes protocolos:

4.359 SSL 3;

4.360 TLS 1.0;

4.361 TLS 1.1;

4.362 TLS 1.2;

4.363 TLS 1.3;

4.364 Deve suportar chaves de 1024 bits, 2048 bits e 4096 bits

4.365 O equipamento deve suportar, no mínimo, as seguintes cifras de criptografia:

4.366 AES_128_CBC;

4.367 AES_256_CBC;

4.368 AES_128_GCM;

4.369 AES_256_GCM;

4.370 Camellia;

4.371 Chacha20;

4.372 Deve implementar o envio de tráfego aberto, sem criptografia, para ferramentas que trabalham em modelo out-of-band (cópia);

4.373 A garantia e todas as licenças devem ser fornecidas com vigência e suporte por 24 (vinte e quatro) meses;

4.374 FUNCIONALIDADE DE OTIMIZAÇÃO DE CÓPIA DE TRÁFEGO PARA FERRAMENTAS, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.375 Deve ser compatível com Network Packet Broker desse Termo de Referência.

4.376 Deve implementar a funcionalidade de envio de cópia de tráfego para ferramentas que trabalham com formato out-of-band (cópia), tais como NDR, NPM etc.

4.377 Os equipamentos, módulos, software e licenças utilizados para essa funcionalidade devem ser todos do mesmo fabricante do Network Packet Broker, facilitando assim a gerência e integração das soluções.

4.378 Deve implementar, para este caso, a funcionalidade de Packet De-Duplication, ou deduplicação de pacotes, através da instalação de licenças e módulos adicionais, se necessário;

4.379 A funcionalidade de Packet De-Duplication deve suportar de-duplicação de pacotes IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o Payload e os

cabeçalhos ethernet.

4.380 A funcionalidade Packet De-Duplication deve detectar pacotes duplicados recebidos em diferentes portas ou módulos do(s) equipamento(s), inclusive se utilizado em modo Mesh/Cluster, detectando pacotes duplicados entre diferentes portas, módulos e equipamentos.

4.381 A funcionalidade Packet De-Duplication deve permitir habilitar ou desabilitar a inspeção de, no mínimo, os seguintes campos para avaliar se é um pacote duplicado ou não:

4.382 IPv4 ToS;

4.383 IPv6 TC;

4.384 Número da Sequência TCP;

4.385 VLAN ID;

4.386 Deve implementar a funcionalidade de Application Aware (App-Aware), que permite compreender uma sessão completa de um fluxo de dados e encaminhar/bloquear todos os pacotes subsequentes desta sessão para as Ferramentas.

4.387 A funcionalidade App-Aware deve suportar a utilização de buffer da sessão, permitindo armazenar, no mínimo, os 20 pacotes iniciais da sessão, para que nos casos onde o padrão da sessão for detectado após o handshake da sessão, todos os pacotes anteriores também sejam encaminhados para as Ferramentas.

4.388 A funcionalidade App-Aware deve suportar a filtragem de tráfego com base na visibilidade da camada de aplicação, permitindo a identificação bidirecional do tráfego na camada 7 do modelo OSI através de funcionalidade de DPI (Deep Packet Inspection).

4.389 Deve suportar a identificação de, no mínimo, 3500 aplicações agrupadas por famílias ou grupos de aplicações tais como YouTube, Whatsapp e Gmail.

4.390 Deve suportar a definição de assinaturas para aplicações customizadas, incluindo protocolos e extensões proprietárias.

4.391 Após a identificação do tráfego com base na aplicação, a solução deve suportar a criação de filtros (regras) de encaminhamento e replicação de tráfego

4.392 A garantia e todas as licenças devem ser fornecidas com vigência e suporte por 24 (vinte e quatro) meses;

4.393 GERÊNCIA CENTRALIZADA - NETWORK PACKET BROKER, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 24 (VINTE E QUATRO) MESES.

4.394 Deverá ser fornecido um software capaz de controlar, administrar, gerenciar e monitorar a solução de Visibilidade.

4.395 O software deverá estar licenciado para, no mínimo, 5 ativos físicos da solução de Visibilidade, e permitir upgrades através da aquisição de licença adicional.

4.396 O software deve ser fornecido em formato de appliance virtual, e deve suportar a instalação em, no mínimo, os seguintes ambientes (que serão fornecidos pela SEMIT / COGEL):

4.397 VMWARE ESXi 7.0 ou superior

4.398 VMWARE NSX-T 3.1.0 ou superior

4.399 NUTANIX AOS 6.5 ou superior

4.400 Possuir gerenciador em um único ponto central para orquestrar todo os elementos físicos, virtuais, em nuvem e containers que compõem o projeto. A solução deve permitir o gerenciamento de todos os appliances componentes da solução;

4.401 A solução deve possuir uma interface gráfica e intuitiva com API abertas para

simples customização de aplicações e integração com produtos de terceiros;

4.402 A solução deve ser capaz de visualizar e gerenciar os dados e métricas coletadas em múltiplos segmentos monitorados em uma única console (centralizada), permitindo desta forma integração, maior segurança, escalabilidade, robustez e disponibilidade da solução.

4.403 Possuir interface gráfica para a criação dos filtros (regras), onde é possível selecionar as portas de Rede e as portas de Ferramentas, independentemente do equipamento físico. Os filtros (regras) criados para estes tráfegos deverão ser aplicados através desta mesma interface Web (HTTPS), facilitando a operação e entendimento dos fluxos.

4.404 A solução deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização;

4.405 A solução deve permitir que os usuários façam "drill down" a partir de visões de alto nível, orientadas a serviços, até visões técnicas com dados detalhados, que auxiliem na análise da causa raiz do problema.

4.406 Deve permitir a criação de topologias da solução de Visibilidade para todos os equipamentos ativos e gerenciáveis.

4.407 Deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas.

4.408 A solução deve permitir o inventário detalhado de atributos dos ativos da solução, atendendo, no mínimo, números seriais, módulos instalados, status do equipamento e versão de software instalado.

4.409 A solução deve permitir o armazenamento das configurações dos dispositivos.

4.410 A ferramenta deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede. O agendamento deve ter periodicidade mínima de um dia.

4.411 Deve permitir o upgrade do sistema operacional ou Boot Prom dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente.

4.412 A ferramenta deve permitir a execução do reset dos dispositivos.

4.413 A ferramenta deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição.

4.414 A solução deverá possuir dashboards com, no mínimo, as seguintes informações:

4.415 Total de portas que estão perdendo pacotes;

4.416 Total de portas acima do limite de utilização, tanto portas de Rede como portas de Ferramenta;

4.417 TOP portas com maior utilização;

4.418 Visualização simplificada de todos os filtros (regras) aplicados, indicando as portas de Redes e Ferramentas;

4.419 Requisitos de Logs:

4.420 A solução deve possuir ferramenta para acompanhamento e análise de eventos de logs;

4.421 Deve permitir a geração de log externo (syslog) para integração com soluções de SIEM;

4.422 A solução deverá gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes. Os registros de logs devem conter a identificação do evento, data e hora, identificação do usuário, identificação do dispositivo e endereço IP do dispositivo ou permitir que estas informações sejam correlacionadas com o mecanismo de SIEM como por exemplo QRadar IBM e Splunk;

4.423 A garantia e todas as licenças devem ser fornecidas com vigência e suporte por 24 (vinte e quatro) meses;

4.424 SERVIÇO ESPECIALIZADO PARA INSTALAÇÃO, MIGRAÇÃO E SUPORTE PREVENTIVO/CORRETIVO -24 (VINTE E QUATRO) MESES – GRUPO 1 – ITENS 1, 2 ,3, 4, 5 e 9:

4.425 Serviço de suporte especializado para instalação, ajustes, configurações e migrações da solução a ser fornecida;

4.426 Além do serviço inicial de instalação e configuração, neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução, seja este corretivo ou preventivo, bem como a transferência de conhecimento hands-on;

4.427 Num prazo de até 10 (dez) dias úteis após a conclusão de instalação da solução ofertada, a contratada deverá fornecer documentação final contendo os manuais de instalação, configurações e utilização. A documentação deverá ser aprovada pela contratante, caracterizando a conclusão dos serviços;

4.428 Para prestação destes serviços, a CONTRATADA deverá empregar funcionários devidamente qualificados na utilização desse tipo de ferramenta;

4.429 O serviço em questão deve atuar em conjunto com o suporte especializado do fabricante para atuação na manutenção e aplicação das melhores práticas no ambiente;

4.430 A CONTRATADA deverá prover equipe técnica especializada própria para atuar nas demandas da CONTRATANTE durante o contrato vigente.

4.431 TREINAMENTO OFICIAL – Grupo 1

4.432 Deverão ser fornecidos vouchers para treinamento oficial com especialista devidamente credenciado pelo fabricante

4.433 Os vouchers devem permitir que a CONTRATANTE selecione os treinamentos e certificações da solução contratada, de acordo com sua demanda de capacitação dá por pessoa durante toda a vigência do contrato, respeitando a quantidade máxima de vouchers;

4.434 O treinamento poderá ser realizado de forma presencial ou remota, de acordo com as medidas sanitárias e legais vigentes durante o período de realização;

4.435 O treinamento deverá ser apresentado no idioma Português do Brasil;

4.436 Durante o treinamento, devem ser fornecidos os materiais necessários para que o participante possa consultar e estudar;

4.437 Os laboratórios e infraestruturas necessárias para realização do treinamento devem ser de responsabilidade da CONTRATADA, permitindo que os participantes apenas utilizem um computador para acessar o ambiente;

4.438 Ao final do treinamento, o voucher fornecido deverá permitir que o participante do treinamento realize uma prova de comprovação dos conhecimentos adquiridos e, caso seja aprovado, deverá receber a certificação de especialista por parte do fabricante;

4.439 A certificação fornecida ao fim do treinamento e aprovação deve ser válida por, pelo menos, 1 ano;

5 ESPECIFICAÇÕES TÉCNICAS DETALHADAS – Grupo 2

5.0 SOLUÇÃO DE MICROSSEGMENTAÇÃO, VISIBILIDADE E PROTEÇÃO DE REDE, BASEADA EM SOFTWARE, PARA CONTROLE DE MOVIMENTAÇÃO LATERAL EM AMBIENTE CORPORATIVO DE SERVIDORES.

5.1 O licenciamento da plataforma deverá ser por ativo protegido, sendo este um dos abaixo:

5.2 Servidores Fisícos (Bare Metal), Virtuais, Cloud (Workloads)

5.3 Toda a solução deverá ser do mesmo fabricante, sem qualquer tipo de customização não autorizada pelo mesmo;

5.4 O gerenciamento da solução deve ser 100% em nuvem e totalmente dedicado para este órgão;

5.5 A solução deve prover no mínimo 99.5% de disponibilidade no nível de serviço;

5.6 A solução SaaS deverá estar hospedada primariamente em Datacenter localizado em território brasileiro, podendo utilizar outro país como contingência;

5.7 Toda a solução deverá ser gerenciada por uma console única de gerência centralizada, para todos os tipos de ativos especificados anteriormente. Serão aceitas exceções em casos de integrações com soluções de terceiros, quando especificado;

5.8 Deverá ser oferecido retenção mínima de 30 dias para todos os dados enviados para a console, incluindo os Fluxos de Dados;

5.9 Não deverá ser necessário qualquer parada (downtime) dos servidores ou aplicações, incluindo, mas não se limitando:

5.10 Reinício (Reboot) dos ativos, sejam servidores, estações de trabalho ou nodes;

5.11 Alteração de IPs, Nomes, configurações de rede em geral, dos ativos;

5.12 Alteração da infrastrutura de rede, seja ela física ou virtual;

5.13 A solução deverá prover, sem custo adicional e de forma nativa, Feeds de Ameaça (Threat Feeds) possuindo, no mínimo, IPs, Domínios e HASHs maliciosos.

5.14 Os Feeds deverão ser dos próprios fabricantes, podendo utilizar também listas de terceiros;

5.15 A solução deverá suportar IPv4 e IPv6;

5.16 Deve ser capaz de monitorar TODOS os fluxos de tráfego do Datacenter: Leste-Oeste (servidor-servidor) e Norte-Sul (rede cliente-servidor ou servidor-externa, ou seja, internet). Para esclarecer, a solução deve monitorar os fluxos de tráfego de todos os ativos que possuem agentes instalado, incluindo também entre máquinas virtuais em execução no mesmo hipervisor, ativos de tipos diferentes, comunicação entre nuvem pública com datacenter privado, entre outros

5.17 A solução também deverá permitir a criação de regras de filtragem de comunicação entre distintos tipos de ativos, bem como entre distintos tipos de ambientes;

5.18 A solução deverá manter registro de todos os Fluxos de Ativos, incluindo os que não foram bloqueados bem como aqueles que falharam (ex.: Timeout);

5.19 Toda a comunicação interna entre os componentes da solução deve ser completamente criptografada e autenticada;

5.20 A solução deverá possuir nos mínimos as seguintes certificações de segurança: ISO 27001, ISO 27018 e SSAE 16 Type 2 (SOC2);

5.21 Deverão ser entregues todos os componentes de hardware necessários para o correto funcionamento da solução;

5.22 ARQUITETURA DA SOLUÇÃO

5.23 A solução deverá ser entregue em modelo SaaS, podendo ser utilizada sem qualquer componente OnPremisses, com exceção dos agentes instalados nos ativos protegidos;

5.24 A Console de Gerenciamento deverá ser única e centralizada para toda a solução;

5.25 Para garantir a segurança dos dados desta organização, o ambiente em nuvem deverá ser dedicado para este órgão. Nenhuma informação deverá ser compartilhada, incluindo os IPs e FQDNs de acesso da Console de Gerenciamento, bem como de todos os outros componentes na nuvem do fabricante da solução;

5.26 Deverá ser possível implementar Relays de comunicação internos, para centralizar a comunicação dos agentes. Esse relay será responsável por receber a comunicação dos agentes e somente ele enviar para a Console Centralizada em nuvem;

5.27 Os Relays poderão ser instalados também em nuvem pública ou privada;

5.28 Caso seja necessário, deverão ser licenciados no mínimo 50 Relays Internos;

5.29 Os Relays deverão trabalhar tanto em Alta Disponibilidade (HA), quando balanceamento (Load Balance) entre eles. Não deverá ser necessário nenhuma solução de terceiros para estas funcionalidades

5.30 Os Relays deverão ser em modelo de Virtual Appliance, compatível no mínimo com:

5.31 VMware;

5.32 Hyper-V;

5.33 AWS;

5.34 Azure;

5.35 GCP;

5.36 OCI;

5.37 A solução deverá utilizar agentes instalados nos ativos protegidos, responsável por coletar os fluxos de dados e garantir a aplicabilidade das regras configuradas;

5.38 Os agentes da solução deverão ser uma implementação de Firewall do próprio fabricante, não utilizando o Firewall nativo do Sistema Operacional;

5.39 Caso os agentes dependam do Firewall do Sistema Operacional, deverão atender os seguintes requerimentos mínimos:

5.40 Deverá estender as capacidades técnicas do Firewall do Sistema Operacional, não se limitando somente a versão nativamente existente, devendo atender aos itens técnicos deste documento;

5.41 Deverá possuir controles nativos da solução que evitem alteração nas políticas definidas pelo administrador da solução de micro segmentação;

5.42 Deverá possuir controles nativos que impeçam a parada do Firewall do Sistema Operacional;

5.43 Bloquear caso o administrador da rede, ou do sistema operacional, tente efetuar alterações manuais nas regras de firewall diretamente no próprio Sistema Operacional;

5.44 Bloquear caso outra solução, como um Antivirus ou EDR, tente efetuar a parada ou desinstalação do Firewall nativo do sistema operacional;

5.45 Bloquear a tentativa de parada, desinstalação ou comprometimento do Firewall nativo do Sistema Operacional em casos de ataques;

5.46 O Fabricante da solução de Micro Segmentação deverá garantir a atualização, ou mecanismos de contorno/proteção, em caso de conhecidas e/ou publicação de novas vulnerabilidades existente no Firewall nativo do Sistema Operacional;

5.47 Os agentes deverão possuir nativamente controle de consumo de CPU e Memória RAM, podendo ser configurável, mas não consumindo mais que 5% nos ativos instalados;

5.48 Possuir coletores com a capacidade de receber flow de rede através de dispositivos físicos, como Switches e Roteadores, sendo compatível no mínimo com os protocolos: Netflow 5 and 9, IPFix, and sFlow;

5.49 Possuir coletor dedicado com a capacidade de receber flows de VMware ESX, através de dados enviados de um Span Port de um switch do tipo VSS (Virtual Standard Switch) ou VDS (vSphere Distributed Switch);

5.50 Possuir coletor dedicado com a capacidade de receber flows de um Span Port de um Switch Fisico, ou um Network TAP;

5.51 Possuir coletor dedicado com a capacidade de receber flows do tipo IPFix, provenientes do F5 BigIP;

5.52 Todos os coletores deverão ser em modelo de Virtual Appliance;

5.53 As informações recebidas pelos Coletores deverão ser representadas em forma gráfica na Console de Gerenciamento;

5.54 A solução deverá possuir de forma nativa Feed de Ameaças (Threat Feeds), do próprio fabricante, possuindo no mínimo informações sobre Domínios, IPs e HASHs maliciosos;

5.55 A solução deverá possuir APIs abertas e documentadas;

5.56 A solução deve possuir, no mínimo, conectores para a seguintes nuvens públicas:

5.57 Amazon Web Services (AWS)

5.58 Microsoft Azure

5.59 Google Cloud Platform (GCP)

5.60 Oracle Cloud (OCI)

5.61 A solução deve possuir, no mínimo, conectores para a seguintes soluções:

5.62 VMware VSphere;

5.63 MS Active Directory;

5.64 F5;

5.65 OpenStack;

5.66 Deve ser capaz de ser implantado em vários segmentos de rede (VLANs), independente do equipamento utilizado para controlar a VLAN;

5.67 A solução deverá possuir a capacidade de Etiquetamento de todos os ativos, incluindo os que possuem agentes ou outros ativos sem agente, mas que se comunicaram ou receberam comunicação de um ativo protegido pela solução;

5.68 Deve ser capaz de detectar e rotear conexões com falha para um servidor dedicado de "Honeypot, podendo ser do mesmo fabricante ou de terceiros, desde que entregue em conjunto com a solução;

5.69 Os agentes deverão ser compatíveis com Microsoft Windows, Linux e Unix.

5.70 CONSOLE DE GERENCIAMENTO

5.71 A console de gerenciamento deverá ser única para toda a solução de micro segmentação;

5.72 Ter a capacidade de gerenciar todos os tipos de ativos em uma única console;

5.73 Ter a capacidade de visualizar os fluxos de dados e configurar as políticas de segurança em uma única console;

5.74 Possuir um Dashboard com as principais informações referentes ao ambiente;

5.75 Ter a capacidade de visualizar em modo gráfico, através de mapas, os fluxos de dados do ambiente;

5.76 Ser possível visualizar de forma agregada o fluxo de dados, de forma gráfica, de um período de tempo, como 30 dias por exemplo;

5.77 Visualizar todos os ativos protegidos, incluindo informações como Nome, Sistema Operacional, Número de CPUs, IP e MAC Address;

5.78 Ter a capacidade de visualizar todas as etiquetas associadas a um único dispositivo;

5.79 Ter a capacidade de visualizar todos os ativos para uma única etiqueta;

5.80 Deve possuir uma área especifica para visualizar todos os fluxos de comunicação de rede coletados no ambiente;

5.81 Deve ser possível filtrar os fluxos de comunicação de dados, no mínimo em:

5.82 Bloqueado, Permitido, não foi possível o bloqueio;

5.83 Origem: por etiqueta e nome do ativo;

5.84 Destino: por etiqueta e nome do ativo;

5.85 Comunicações com Origem ou Destino para a Internet;

5.86 Pelo nome do conjunto de regras de proteção aplicado no ambiente;

5.87 Porta e Protocolo;

5.88 Período de tempo;

5.89 Por processo utilizado da comunicação;

5.90 Ser possível criar novas etiquetas e gerenciar etiquetas existentes;

5.91 Exportar as etiquetas, no mínimo em CSV ou XLS;

5.92 Ter a capacidade, através de interface gráfica na própria console, de monitorar a saúde de todos os componentes da solução, no mínimo para os agentes, coletores e servidores de Relay.

5.93 Ter a capacidade, através de interface gráfica na própria console, de parar e reiniciar os componentes da solução, no mínimo para os agentes, coletores e servidores de Relay;

5.94 Ter a capacidade de atualizar os agentes instalados nos ativos de forma centralizada pela própria console, sem necessitar de execução manual no ativo ou de uso de scripts;

5.95 Deve possuir Logs de Auditoria, para no mínimo:

5.96 Autenticação do usuário: Com sucesso e falha de autenticação

5.97 Política de Segmentação: Criação e alteração de políticas, bem como a ação de desabilitar a política;

5.98 Etiquetas: Criação e alteração;

5.99 Logs: Quem consultou os logs;

5.100 Os Logs de Auditoria devem conter, no mínimo: O dia, hora, Ação Executada, Nome do usuário, IP de Origem e Descrição;

5.101 Deve ser possível gerenciar os usuários com acesso a solução, não havendo limites para o número de usuários existentes;

5.102 Deve possuir integração com sistemas de diretório para integração de autenticação. Deve ser compatível com mínimo com LDAP e SAML 2.0;

5.103 Deve suportar autenticação Kerberos;

5.104 Deve ser possível criar usuários locais, e gerenciar os usuários existentes. Deve permitir alterar a senha do usuário utilizando uma nova senha Temporária de alteração obrigatória no primeiro login;

5.105 Deve suportar segundo fator de autenticação;

5.106 Possuir níveis de permissões diferentes para os usuários, no mínimo com as seguintes características:

5.107 Administrador da solução;

5.108 Somente Leitura;

5.109 Somente visualização dos Incidentes;

5.110 Administração das Políticas;

5.111 Deve ser possível configurar quais etiquetas o usuário possui permissão;

5.112 Ser possível verificar todos os incidentes gerados pela solução diretamente na própria console de administração;

5.113 Ser possível filtrar os incidentes no mínimo por Severidade, Tipo, Etiquetas, Nome do Ativo e período de tempo;

5.114 Deve possuir mecanismo de busca dos incidentes;

5.115 Deve ser possível customizar o nível de criticidade dos incidentes;

5.116 Deve ser possível desabilitar o uso de dados de Reputação, bem como habilitar ou desabilitar o envio de informações de IoC para o fabricante da solução;

5.117 Deve ser possível trabalhar com múltiplos sites, em console única e que permitam aos usuários aplicar seletivamente políticas e regras a um conjunto de ativos nessa localização;

5.118 Deve ser possível gerenciar a administração de políticas em vários sites/divisões gerenciando os escopos dos usuários por site;

5.119 Deve ser possível ao administrador total autonomia para criar, modificar e excluir regras, além de visualizar todos os logs para Ativos atribuídos aos seus sites;

5.120 AGENTES

5.121 A solução deverá possuir agentes instalados nos ativos protegidos;

5.122 Os agentes deverão ser compatíveis com as seguintes plataformas, no mínimo:

5.123 Windows Server: 2000 SP4, 2003 SP2 (32 e 64 bits), 2008 (32 bits), 2008 R2, 2012, 2016, 2016 Core, 2019 e 2022;

5.124 Windows Desktop: XP SP3, Vista SP1 (32 bits), Vista SP2 (64 bits), 7 (32 e 64 bits), 8 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11;

5.125 MacOS Catalina, Bug Sur, Monterey e Ventura

5.126 Red Hat Linux: 4, 5, 5.1, 5.2 até 5.11, 6, 7 e 8 (todos 64 bits);

5.127 CentOS Linux: 5.2 (32 bits), 5.2 até 5.11 (64 bits), 6 até 9 (64 bits);

5.128 Oracle Linux: 5.2 até 5.11, 6 até 9 (todos 64 bits);

5.129 Alma 8 e 9 (64bits)

5.130 Amazon Linux;

5.131 Amazon Linux 2;

5.132 Ubuntu Linux: 12.04 até 22.04 LTS (todos 64 bits);

5.133 Debian Linux: 7.5 até 12 (todos 64 bits);

5.134 SUSE Linux: 11, 12 e 15 (todos 64 bits);

5.135 HP-UX: 11.23 e 11.31;

5.136 Solaris: 10.8 até 10.11 (x86_64 e SPARCv9), 11 até 11.4 (x86_64 e SPARCv9);

5.137 AIX: 6.1, 7.1, 7.2 e 7.3;

5.138 FreeBSD: 11.3 e 12.1 (x86_64);

5.139 Rocky 8 e 9 (64bits)

5.140 Os agentes deverão consumir no máximo 5% de CPU e Memória do ativo instalado, podendo este valor ser configurado nativamente na própria console de Gerenciamento;

5.141 Os agentes deverão ser capazes de coletar informações do ativo, como flows de rede, e executar as políticas de proteção;

5.142 As políticas de proteção deverão permanecer em execução mesmo que o ativo não tenho acesso ao Relay ou a Console de Gerenciamento;

5.143 Os agentes deverão armazenar os Logs de Fluxo de Dados e Incidentes mesmo que o ativo não tenho acesso ao Relay ou a Console de Gerenciamento;

5.144 Os agentes da solução deverão ser uma implementação de Firewall do próprio fabricante, não utilizando o Firewall nativo do Sistema Operacional;

5.145 Caso os agentes não sejam uma implementação nativa de Firewall e dependam do Firewall do Sistema Operacional, deverão atender os seguintes requerimentos mínimos:

5.146 Deverá estender as capacidades técnicas do Firewall do Sistema Operacional, não se limitando somente a versão nativamente existente, devendo atender aos itens técnicos deste documento;

5.147 Deverá possuir controles nativos da solução que evitem alteração nas políticas definidas pelo administrador da solução de micro segmentação;

5.148 Deverá possuir controles nativos que impeçam a parada do Firewall do Sistema Operacional;

5.149 Bloquear caso o administrador da rede, ou do sistema operacional, tente efetuar alterações manuais nas regras de firewall diretamente no próprio Sistema Operacional;

5.150 Bloquear caso outra solução, como um Antivirus ou EDR, tente efetuar a parada ou desinstalação do Firewall nativo do sistema operacional;

5.151 Bloquear a tentativa de parada, desinstalação ou comprometimento do Firewall nativo o Sistema Operacional em casos de ataques;

5.152 O Fabricante da solução de Micro Segmentação deverá garantir a atualização, ou mecanismos de contorno/proteção, em caso de conhecidas e/ou publicação de novas vulnerabilidades existente no Firewall nativo do Sistema Operacional;

5.153 Deverá suportar o uso do agente da solução em conjunto com o Firewall Nativo do Sistema Operacional, ou de terceiros, exceto em casos de Limitação do Sistema Operacional;

5.154 Os agentes deverão capturar todos os Fluxos de Dados nos ativos instalados e enviar para a console de gerenciamento.

5.155 As informações capturadas pelo agente deverão conter no mínimo:

5.156 IP de Origem e Destino;

5.157 Hostname de Origem e Destino;

5.158 Porta e Protocolo;

5.159 Quantidade de conexões;

5.160 Hora e Data;

5.161 Informações do processo/binário responsável pela comunicação, na origem e destino;

5.162 Caminho do binário no ativo;

5.163 Nome do Serviço do Windows (Ex.: BITS) responsável pela comunicação, quando este for executado em um processo padrão (Ex.: SVCHost.exe);

5.164 Usuário que executou o processo;

5.165 FQDN ou IP, quando for um acesso com origem ou destino para Internet;

5.166 A instalação do agente não deverá requer qualquer tipo de parada no Sistema Operacional, incluindo reiniciar (Reboot);

5.167 A instalação do agente não deverá requerer qualquer tipo alteração no ativo, como mudança de IP, Hostname, ou instalação de software que possam comprometer o funcionamento normal da aplicação;

5.168 Serão aceitas soluções que não se utilizem somente de agentes para efetuar todos os controles requeridos.

5.169 Serão aceitas soluções complementares para atender os requerimentos deste documento, desde que suportadas pelos mesmos SLAs e pelo único vencedor desta concorrência;

5.170 Caso a solução não utilize somente agentes para efetuar todos os controles requeridos, deverão ser entregues todos os hardware e/ou softwares necessários, com o mesmo quantitativo de licenças, para atendimento dos itens;

5.171 Os agentes deverão ter a capacidade de coletar informações dos ativos que estão instalados, como exemplo, mas não se limitando: Número de CPUs, processos em execução, usuários pertencentes ao grupo de administrador local, softwares instalados, uptime do sistema, ativos com um determinado software instalado, entre outros;

5.172 **VISIBILIDADE**

5.173 A solução deverá prover visibilidade de toda a comunicação de rede de forma gráfica, através de um mapa de rede;

5.174 Deve permitir navegar facilmente pelo mapa e focar em parte específica do data center ou aplicativos específicos;

5.175 Deve possuir, no mapa de rede, filtros de inclusão e exclusão, permitindo filtrar no mínimo:

5.176 IP;

5.177 Porta;

5.178 Aplicação, Binário e Serviço;

5.179 Nome do Ativo;

5.180 Tipo de Conexão - Estabelecida, falhada (time out), bloqueada e as que violaram uma política;

5.181 Internet - Com Origem e Destino da Internet;

5.182 Usuário que iniciou o processo;

5.183 Ser possível criar diferentes mapas de rede, determinando o período de tempo e aplicando filtros conforme item anterior;

5.184 Deve ser possível remover Mapas de Fluxo de Dados;

5.185 Deve reter os fluxos de dados por um mínimo de 45 dias, sendo possível criar ou visualizar os mapas utilizando períodos históricos;

5.186 A tela do Mapa de Dados deve possuir mecanismo de busca;

5.187 O mapa de dados deverá apresentar informações de comunicação em Camada 4 e Camada 7;

5.188 Deverá ser possível aplicar Etiquetas diretamente na tela do Mapa de Dados, de forma pontual (único ativo) ou para vários ativos ao mesmo tempo;

5.189 Deverá ser possível verificar as Etiquetas aplicadas a um ativo diretamente da tela do Mapa de Dados;

5.190 Ser possível identificar a quantidade de vezes que uma determinada comunicação aconteceu em um período de tempo;

5.191 Ser possível, no mapa de dados, obter informações do processo que efetuou uma determinada comunicação, possuindo no mínimo informações do Caminho do Binário no Ativo, o PID, o HASH, o usuário que executou o processo e a linha de comando executada;

5.192 Deve ser possível, no mapa de dados, visualizar as comunicações de todos os ativos do ambiente, máquina a máquina;

5.193 Deve ser possível, no mapa de dados, agrupar os ativos através das etiquetas existentes no ambiente, permitindo ainda hierarquizar em subgrupos;

5.194 Deve registrar e apresentar todos os fluxos de comunicação do datacenter, em formato de tabela, juntamente com informações contextuais e detalhadas sobre as cargas de trabalho e aplicativos (processos) de comunicação;

5.195 Deve fornecer recursos de filtragem (Ip/Porta/Processo/Origem/Destino/Usuário que iniciou a comunicação) se a comunicação foi estabelecida/bloqueada;

5.196 Deve descobrir automaticamente qualquer novo fluxo de comunicação em tempo real;

5.197 Deve ser possível filtrar os fluxos de dados por um conjunto de regras aplicados no ambiente;

5.198 Deve ser possível exportar os fluxos de dados no mínimo em CSV;

5.199 Deve ser possível visualizar todos os ativos, através da console, obtendo informações da primeira vez que foi visto e a última vez que o ativo se comunicou com a console;

5.200 Deverá ser possível etiquetar ou aplicar TAGs nos ativos do ambiente, ativos com agentes e sem agentes, para utilizar tanto na visualização, em políticas bem como em filtros;

5.201 A etiquetas deverão seguir um modelo de Categoria e Valores, por exemplo Ambiente / Produção, ou de forma similar onde é possível incluir valores diferentes para uma mesma categoria;

5.202 As etiquetas deverão ser criadas através da própria console de gerenciamento, no mínimo das seguintes formas:

5.203 De forma manual, adicionando diretamente ao dispositivo, podendo inclusive ser através do mapa de fluxo de dados;

5.204 Através de Inteligência Artifical - A solução deverá sugerir Etiquetas baseadas nas aplicações existentes no dispositivo;

5.205 Dinâmicamente - Ex: Todo dispositivo que o nome contém PROD, ou que estão na subrede 10.0.0.0/8, aplicar Etiqueta Ambiente:

5.206 Produção Através de integração com CMDB - Coletar os dados diretamente da solução de CMDB utilizada;

5.207 Através de Integração com sistemas que já possuem TAGs - Como VMWare VCenter, Nuvens públicas (AWS, GCP, Azure, OCI) e CSV.

5.208 Através de APIs públicas

5.209 Não deve existir um limite no tipo e/ou nome de Etiquetas a serem criadas na solução, para as categorias e para os valores;

5.210 Deverá ser possível agrupar etiquetas em Grupos de Etiquetas, para uso nas políticas e outras partes da solução;

5.211 Deverá ser registrado em Log toda a criação, remoção ou modificação das etiquetas, informando no mínimo o usuário responsável, hora e data e a etiqueta alterada. Esses logs deverão ser acessíveis através da própria console de gerenciamento;

5.212 Deverá ser possível aplicar uma etiqueta a um único dispositivo, e a um conjunto de dispositivos;

5.213 A console de gerenciamento deverá possuir uma área específica de informações dos ativos que devem apresentar todas as Etiquetas aplicadas ao ativo;

5.214 As etiquetas poderão ser utilizadas no Mapa de Visualizações de Fluxo de Dados e nas criações de políticas;

5.215 Deverá ser possível hierarquizar as etiquetas, sem restrições, para visualização agrupada com subníveis no mapa de fluxo de dados.

5.216 A hierarquização de etiquetas poderá utilizar qualquer etiqueta do ambiente, e não ter limitador do número de níveis

5.217 Deverá apresentar no mapa de fluxo de dados os dispositivos gerenciados e não-gerenciados pela solução;

5.218 **MICRO SEGMENTAÇÃO E SEGURANÇA DO AMBIENTE**

5.219 Deve fornecer a capacidade de criar, gerenciar e monitorar políticas de tráfego Leste-Oeste e Norte-Sul flexíveis até o nível de uma única carga de trabalho e aplicativo (processo ou serviço do MS Windows);

5.220 Deve permitir criar e monitorar políticas de comunicação de aplicativo a partir do mapa de visualização;

5.221 Deve suportar regras definidas sobre grupos de ativos de acordo com sua função ou etiquetamento;

5.222 Deve possuir no mínimo 3 (três) tipos de regras: Bloqueio, Permissão e Alerta;

5.223 Deve permitir trabalhar tanto com Whitelist como Blacklist, de forma independente;

5.224 Deve permitir criar regras de micro segmentação utilizando os seguintes parâmetros como Origem e Destino:

5.225 Etiquetas e Grupo de Etiquetas

5.226 Ativo (nome do ativo)

5.227 IP/Subrede

5.228 Aplicação / Processo do Windows (Ex.: BITS)

5.229 Grupo de usuários

5.230 FQDN

5.231 Internet (Comunicação vindo da Internet / Rede Interna)

5.232 Qualquer (Any)

5.233 Deve permitir criar regras de Bloqueio, Permissão e Alerta utilizando a Porta e Protocolo (TCP/UDP), incluindo ICMP;

5.234 Deve ser possível criar regras de bloqueio, permissão e alerta, de forma independente. Por exemplo, criar somente uma regra para alertar caso o IIS.EXE de um servidor se comunique com o SQL.EXE de outro servidor;

5.235 Deve ser possível criar regras somente de bloqueio, sem precisar fazer uma Whitelist da aplicação. Por exemplo, com uma única regra bloquear todos os servidores de Banco de Dados de receber comunicação da Internet;

5.236 Deve ser possível agrupar ou nomear um conjunto de regras com a mesma finalidade, para facilitar o gerenciamento, visualização e filtros por esse agrupamento;

5.237 Ser possível desabilitar uma regra, ou um conjunto de regras, sem a necessidade de excluir da console;

5.238 Possuir filtros de informações no gerenciamento das regras do ambiente;

5.239 Ser possível identificar e filtrar as regras pelo usuário que a criou;

5.240 As regras devem ser publicadas manualmente para os ativos, podendo inclusive escolher se serão aplicadas todas as regras ou um conjunto específico baseado no nome do agrupamento;

5.241 Deve salvar as revisões de política e permitir a reversão para versões anteriores;

5.242 A solução deve possuir nativamente modelos (templates) pré-definidos para aplicações conhecidas de mercado (Ex.: Active Directory), tendo o catálogo disponibilizado na própria console de gerenciamento;

5.243 Deve possuir nativamente modelos (templates) pré-definidos para políticas de Prevenção de Ransomware;

5.244 A solução deve sugerir automaticamente aplicação de políticas de micro segmentação para as aplicações existentes no ambiente;

5.245 Deve sugerir a criação de regras de forma automática com base no fluxo histórico de comunicação das aplicações (mínimo de 30 dias como base de pesquisa);

5.246 Deve poder sugerir políticas automaticamente de acordo com os dados coletados;

5.247 A solução deve utilizar Inteligência Artificial para analisar fluxos de dados históricos (mínimo de 30 dias) e sugerir políticas de segmentação para qualquer aplicação do ambiente;

5.248 Deve permitir incluir na política a identidade do usuário autenticado no ativo. Será aceito para esta funcionalidade a integração com outra solução do mesmo fabricante, desde que seja entregue o quantitativo de licenças necessário para o correto funcionamento;

5.249 Deve ser possível criar políticas com Lógicas de E OU;

5.250 Durante a criação de políticas, ao ser selecionado a categoria de Aplicação / Processo do Windows, deverão aparecer automaticamente todos os processos já identificados no ambiente pelo agente ou pelo Relay. Ainda deverá ser possível adicionar manualmente um novo processo, que ainda não se comunicou no datacenter;

5.251 A solução deverá permitir a inclusão de listas de FQDNs, através de importação de arquivo, para serem utilizadas durante a consulta DNS em bloqueio ou liberação de acesso a sites específicos;

5.252 Deve ter a capacidade de isolar uma máquina da rede, ou um grupo de máquinas, com uma única regra;

5.253 A solução deverá permitir a criação de políticas baseado nos Feeds de Ameaças (Threat Intel) da própria plataforma, possibilitando alertar ou bloquear a comunicação de um Binário, IP ou Domínio malicioso;

5.254 Deve ser possível bloquear e permitir uma comunicação efetuada pela mesma porta e protocolo utilizando binários diferentes.

5.255 Deve permitir a criação de regras com usuários em ambientes VDI/Terminal/Citrix de forma a garantir que apenas determinados grupos do Active Directory possam chegar a um determinado endereços e/ou aplicações na rede;

5.256 Deve permitir a combinação de regras utilizando máquina/usuário/processo de origem e serviço no destino, exemplo: no servidor/estação apenas os usuários do grupo do AD de CRM utilizando a aplicação do ORACLECRM.EXE podem chegar ao servidor de Front End da Aplicação do Oracle;

5.257 Deve informar ao usuário o impacto das regras criadas no fluxo de comunicação de forma visual, simulando o impacto das regras no fluxo de comunicações;

5.258 Em sistemas operacionais Windows, deve permitir criar regras utilizando não somente o processo como também o serviço. Por exemplo, o serviço BITS pode acessar o domínio *.microsoft.com, sem a necessidade de bloquear o SVCHOST.exe por completo;

5.259 Não deverá ser necessário criar regras especificas por sistema operacional diferentes, em qualquer um dos casos. Por exemplo, uma regra criada utilizando binários e serviços poderá conter informações de Linux e Windows e ser aplicada em ambos os Sistemas Operacionais, onde o agente será responsável por ignorar o que não for referente a aquela versão de sistema operacional;

5.260 Deve detectar, analisar e relatar suspeitas de tentativas de movimento lateral;

5.261 Deve ser capaz de permitir tipos de eventos personalizáveis, prioridade e gravidade para tipos de eventos individuais;

5.262 Deve permitir editar listas de indicadores confiáveis;

5.263 Deve permitir a definição de políticas de inspeção - tráfego e cargas de trabalho que devem ser completamente ignoradas, bem como tráfego e cargas de trabalho que devem ser ignoradas na investigação de fraude dinâmica de ameaças;

5.264 Deve alertar sobre a violação da política e fornecer informações detalhadas sobre a violação da conexão, indicando inclusive qual processo iniciou a comunicação;

5.265 Deve possuir mecanismo de reputação de hash para todo e qualquer processo que tente se comunicar com a rede;

5.266 Deve permitir a integração com fontes externas de informação para aumentar a base de detecção de hashes;

5.267 Deve possuir mecanismo de reputação de DNS e validar toda e qualquer tentativa de resolução de nomes nos ativos protegidos pela solução;

5.268 Deve possuir mecanismo de reputação de IP, para evitar comunicações de IP's sabidos como maliciosos da internet;

5.269 É necessário oferecer a opção de verificar todos os processos de comunicação como parte de malware conhecido por um serviço de reputação incluído.

5.270 DETECÇÃO AVANÇADA DE AMEAÇAS

5.271 Deve detectar, analisar e relatar suspeitas de tentativas de movimento lateral;

5.272 Deve ser capaz de detectar e rotear conexões que infringiram uma política para um servidor de decepção (também conhecido como "honeypot"), acionado por qualquer tentativa de acessar portas fechadas / filtradas em máquinas reais;

5.273 A solução deverá provisionar dinamicamente um servidor de "honeypot" em tempo real, do próprio fabricante ou através de integração com terceiros. Caso a solução seja de terceiros, deverá ser incluída nesta contratação;

5.274 É necessário usar máquinas reais (e não emulações) como base do servidor de decepção ("honeypot de alta interação"), e os invasores devem poder interagir com o servidor de fraude em todos os níveis.

5.275 Deve ser capaz de apresentar servidores de "honeypot" baseados em Windows e Linux e bancos de dados;

5.276 Deve fornecer isolamento completo do servidor de "honeypot" e impedir que o invasor use o mesmo como plataforma de lançamento para atacar ainda mais os ativos da rede;

5.277 Deve possuir a capacidade de efetuar download de todos os arquivos criados e modificados para análise local do servidor de "honeypot";

5.278 Deve possuir a capacidade de baixar capturas de tela do servidor de decepção do Windows ("honeypot") capturadas durante a interação com um invasor;

5.279 É necessário registrar todas as credenciais tentadas em um servidor de "honeypot";

5.280 Deve oferecer suporte a uma lista configurável de credenciais que concederia ao invasor acesso ao serviço solicitado no servidor de "honeypot";

5.281 Deve suportar um número configurável de tentativas de login antes de conceder ao invasor de força bruta acesso ao serviço solicitado no servidor de "honeypot";

5.282 Deve ser capaz de detectar todas as chamadas do sistema no nível do sistema operacional, bem como a atividade no nível do aplicativo e usuário executando o aplicativo, no servidor de "honeypot";

5.283 Deve ser capaz de detectar a atividade do invasor no servidor de decepção ("honeypot") sem uma maneira razoável de o invasor perceber que está envolvido em um sistema altamente monitorado;

5.284 Deve ser capaz de apresentar a gravação da sessão completa de todas as atividades do invasor no nível do sistema e do aplicativo;

5.285 Deve ser capaz de detectar automaticamente a atividade humana versus ataques automatizados;

5.286 A solução deve possuir mecanismo de consulta instantânea nos dispositivos gerenciados compatível com padrão OSQUERY;

5.287 Deverá ter a capacidade de coletar informações dos ativos com o agente da solução, como exemplo, mas não se limitando: Número de CPUs, processos em execução, usuários pertencentes ao grupo de administrador local, softwares instalados, uptime do sistema, ativos com um determinado software instalado, entre outros;

5.288 Ser capaz de aplicar Etiquetas no ambiente através do resultado de uma consulta e/ou coleta de informações;

5.289 Deverá ser possível agendar estas consultas para execuções contínuas, podendo

inclusive adicionar uma etiqueta automaticamente aos ativos encontrados;

5.290 Deverá ser possível consultar vulnerabilidades nos ativos, e aplicar etiquetas dedicadas aos ativos vulneráveis. Estas etiquetas de vulnerabilidade poderão ser utilizadas no mapa de fluxo de dados e também para criação de políticas;

5.291 SOLUÇÃO DE MICROSSEGMENTAÇÃO, VISIBILIDADE E PROTEÇÃO DE REDE, BASEADA EM SOFTWARE, PARA CONTROLE DE MOVIMENTAÇÃO LATERAL EM AMBIENTES CORPORATIVOS EM CONTAINERS

5.292 O licenciamento da plataforma deverá ser por ativo protegido, sendo este um dos abaixo:

5.293 Nós (Nodes) de Contêineres / Kubernetes;

5.294 Toda a solução deverá ser do mesmo fabricante, sem qualquer tipo de customização não autorizada pelo mesmo;

5.295 O gerenciamento da solução deve ser 100% em nuvem e totalmente dedicado para este órgão;

5.296 A solução deve prover no mínimo 99.5% de disponibilidade no nível de serviço;

5.297 A solução SaaS deverá estar hospedada primariamente em Datacenter localizado em território brasileiro, podendo utilizar outro país como contingência;

5.298 Toda a solução deverá ser gerenciada por uma console única de gerência centralizada, para todos os tipos de ativos especificados anteriormente. Serão aceitas exceções em casos de integrações com soluções de terceiros, quando especificado;

5.299 Deverá ser oferecido retenção mínima de 30 dias para todos os dados enviados para a console, incluindo os Fluxos de Dados;

5.300 Não deverá ser necessário qualquer parada (downtime) dos servidores ou aplicações, incluindo, mas não se limitando:

5.301 Reinício (Reboot) dos ativos, sejam servidores, estações de trabalho ou nodes;

5.302 Alteração de IPs, Nomes, configurações de rede em geral, dos ativos;

5.303 Alteração da infraestrutura de rede, seja ela física ou virtual;

5.304 A solução deverá prover, sem custo adicional e de forma nativa, Feeds de Ameaça (Threat Feeds) possuindo, no mínimo, IPs, Domínios e HASHs maliciosos.

5.305 Os Feeds deverão ser dos próprios fabricantes, podendo utilizar também listas de terceiros;

5.306 A solução deverá suportar IPv4 e IPv6;

5.307 Deve ser capaz de monitorar TODOS os fluxos de tráfego do Datacenter: Leste-Oeste (servidor-servidor) e NorteSul (rede cliente-servidor ou servidor-externa, ou seja, internet). Para esclarecer, a solução deve monitorar os fluxos de tráfego de todos os ativos que possuem agentes instalado.

5.308 A solução também deverá permitir a criação de regras de filtragem de comunicação entre distintos tipos de ativos, bem como entre distintos tipos de ambientes;

5.309 A solução deverá manter registro de todos os Fluxos de Ativos, incluindo os que não foram bloqueados bem como aqueles que falharam (ex.: Timeout);

5.310 Toda a comunicação interna entre os componentes da solução deve ser completamente criptografada e autenticada;

5.311 A solução deverá possuir nos mínimos as seguintes certificações de segurança: ISO 27001, ISO 27018 e SSAE 16 Type 2 (SOC2);

5.312 Deverão ser entregues todos os componentes de hardware necessários para o

correto funcionamento da solução;

5.313 ARQUITETURA DA SOLUÇÃO

5.314 A solução deverá ser entregue em modelo SaaS, podendo ser utilizada sem qualquer componente OnPremisses, com exceção dos agentes instalados nos ativos protegidos;

5.315 A Console de Gerenciamento deverá ser única e centralizada para toda a solução;

5.316 Para garantir a segurança dos dados desta organização, o ambiente em nuvem deverá ser dedicado para este órgão. Nenhuma informação deverá ser compartilhada, incluindo os IPs e FQDNs de acesso da Console de Gerenciamento, bem como de todos os outros componentes na nuvem do fabricante da solução;

5.317 Deverá ser possível implementar Relays de comunicação internos, para centralizar a comunicação dos agentes. Esse relay será responsável por receber a comunicação dos agentes e somente ele enviar para a Console Centralizada em nuvem;

5.318 Os Relays poderão ser instalados também em nuvem pública ou privada;

5.319 Caso seja necessário, deverão ser licenciados no mínimo 50 Relays Internos;

5.320 Os Relays deverão trabalhar tanto em Alta Disponibilidade (HA), quando balanceamento (Load Balance) entre eles. Não deverá ser necessário nenhuma solução de terceiros para estas funcionalidades

5.321 Os Relays deverão ser em modelo de Virtual Appliance, compatível no mínimo com:

5.322 VMware;

5.323 Hyper-V;

5.324 AWS;

5.325 Azure;

5.326 GCP;

5.327 OCI;

5.328 A solução deverá utilizar agentes instalados nos ativos protegidos, responsável por coletar os fluxos de dados e garantir a aplicabilidade das regras configuradas;

5.329 Os agentes da solução deverão ser uma implementação de Firewall do próprio fabricante, não utilizando o Firewall nativo do Sistema Operacional;

5.330 Caso os agentes dependam do Firewall do Sistema Operacional, deverão atender os seguintes requerimentos mínimos:

5.331 Deverá estender as capacidades técnicas do Firewall do Sistema Operacional, não se limitando somente a versão nativamente existente, devendo atender aos itens técnicos deste documento;

5.332 Deverá possuir controles nativos da solução que evitem alteração nas políticas definidas pelo administrador da solução de micro segmentação;

5.333 Deverá possuir controles nativos que impeçam a parada do Firewall do Sistema Operacional;

5.334 Bloquear caso o administrador da rede, ou do sistema operacional, tente efetuar alterações manuais nas regras de firewall diretamente no próprio Sistema Operacional;

5.335 Bloquear caso outra solução, como um Antivirus ou EDR, tente efetuar a parada ou desinstalação do Firewall nativo do sistema operacional;

5.336 Bloquear a tentativa de parada, desinstalação ou comprometimento do Firewall

nativo do Sistema Operacional em casos de ataques;

5.337 O Fabricante da solução de Micro Segmentação deverá garantir a atualização, ou mecanismos de contorno/proteção, em caso de conhecidas e/ou publicação de novas vulnerabilidades existente no Firewall nativo do Sistema Operacional;

5.338 A solução deverá possuir de forma nativa Feed de Ameaças (Threat Feeds), do próprio fabricante, possuindo no mínimo informações sobre Domínios, IPs e HASHs maliciosos;

5.339 A solução deverá possuir APIs abertas e documentadas;

5.340 A solução deve possuir, no mínimo, conectores para a seguintes nuvens públicas:

5.341 Amazon Web Services (AWS)

5.342 Microsoft Azure

5.343 Google Cloud Platform (GCP)

5.344 Oracle Cloud (OCI)

5.345 A solução deve possuir, no mínimo, conectores para a seguintes soluções:

5.346 VMware VSphere;

5.347 MS Active Directory;

5.348 F5;

5.349 OpenStack;

5.350 Deve ser capaz de ser implantado em vários segmentos de rede (VLANs), independente do equipamento utilizado para controlar a VLAN;

5.351 A solução deverá possuir a capacidade de Etiquetamento de todos os ativos, incluindo os que possuem agentes ou outros ativos sem agente, mas que se comunicaram ou receberam comunicação de um ativo protegido pela solução;

5.352 CONSOLE DE GERENCIAMENTO

5.353 A console de gerenciamento deverá ser única para toda a solução de micro segmentação;

5.354 Ter a capacidade de gerenciar todos os tipos de ativos em uma única console;

5.355 Ter a capacidade de visualizar os fluxos de dados e configurar as políticas de segurança em uma única console;

5.356 Possuir um Dashboard com as principais informações referentes ao ambiente;

5.357 Ter a capacidade de visualizar em modo gráfico, através de mapas, os fluxos de dados do ambiente;

5.358 Ser possível visualizar de forma agregada o fluxo de dados, de forma gráfica, de um período de tempo, como 30 dias por exemplo;

5.359 Ter a capacidade de visualizar todas as etiquetas associadas a um único dispositivo;

5.360 Ter a capacidade de visualizar todos os ativos para uma única etiqueta;

5.361 Deve possuir uma área especifica para visualizar todos os fluxos de comunicação de rede coletados no ambiente;

5.362 Deve ser possível filtrar os fluxos de comunicação de dados, no mínimo em:

5.363 Bloqueado, Permitido, não foi possível o bloqueio;

5.364 Origem: por etiqueta e nome do ativo;

5.365 Destino: por etiqueta e nome do ativo;

5.366 Comunicações com Origem ou Destino para a Internet;

5.367 Pelo nome do conjunto de regras de proteção aplicado no ambiente;

5.368 Porta e Protocolo;

5.369 Período de tempo;

5.370 Por container utilizado da comunicação;

5.371 Ser possível criar novas etiquetas e gerenciar etiquetas existentes;

5.372 Exportar as etiquetas, no mínimo em CSV ou XLS;

5.373 Ter a capacidade, através de interface gráfica na própria console, de monitorar a saúde de todos os componentes da solução, no mínimo para os coletores, servidores de Relay e Clusters Kubernetes

5.374 Ter a capacidade, através de interface gráfica na própria console, de parar e reiniciar os componentes da solução, no mínimo para os coletores e servidores de Relay;

5.375 Deve possuir Logs de Auditoria, para no mínimo:

5.376 Autenticação do usuário: Com sucesso e falha de autenticação

5.377 Política de Segmentação: Criação e alteração de políticas, bem como a ação de desabilitar a política;

5.378 Etiquetas: Criação e alteração;

5.379 Logs: Quem consultou os logs;

5.380 Os Logs de Auditoria devem conter, no mínimo: O dia, hora, Ação Executada, Nome do usuário, IP de Origem e Descrição;

5.381 Deve ser possível gerenciar os usuários com acesso a solução, não havendo limites para o número de usuários existentes;

5.382 Deve possuir integração com sistemas de diretório para integração de autenticação. Deve ser compatível com mínimo com LDAP e SAML 2.0;

5.383 Deve suportar autenticação Kerberos;

5.384 Deve ser possível criar usuários locais, e gerenciar os usuários existentes. Deve permitir alterar a senha do usuário utilizando uma nova senha Temporária de alteração obrigatória no primeiro login;

5.385 Deve suportar segundo fator de autenticação;

5.386 Possuir níveis de permissões diferentes para os usuários, no mínimo com as seguintes características:

5.387 Administrador da solução;

5.388 Somente Leitura;

5.389 Somente visualização dos Incidentes;

5.390 Administração das Políticas;

5.391 Deve ser possível configurar quais etiquetas o usuário possui permissão;

5.392 Ser possível verificar todos os incidentes gerados pela solução diretamente na própria console de administração;

5.393 Ser possível filtrar os incidentes no mínimo por Severidade, Tipo, Etiquetas, Nome do Ativo e período de tempo;

5.394 Deve possuir mecanismo de busca dos incidentes;

5.395 Deve ser possível customizar o nível de criticidade dos incidentes;

5.396 Deve ser possível desabilitar o uso de dados de Reputação, bem como habilitar ou

desabilitar o envio de informações de IoC para o fabricante da solução;

5.397 Deve ser possível trabalhar com múltiplos sites, em console única e que permitam aos usuários aplicar seletivamente políticas e regras a um conjunto de ativos nessa localização;

5.398 Deve ser possível gerenciar a administração de políticas em vários sites/divisões gerenciando os escopos dos usuários por site;

5.399 Deve ser possível ao administrador total autonomia para criar, modificar e excluir regras, além de visualizar todos os logs para Ativos atribuídos aos seus sites;

5.400 AGENTES

5.401 Os agentes da solução deverão operar como um DaemonSet diretamente no Nó do Cluster;

5.402 Deve coletar todos os fluxos de dados de comunicação, entre PODs, bem como com origem e/ou destino de infraestrutura não baseada em micro serviço;

5.403 Deverá ser compatível com as seguintes Plataformas de Containêres:

5.404 EKS;

5.405 AKS;

5.406 GKE;

5.407 OpenShift 3.x/4.x;

5.408 RKE

5.409 ARO4.2.4.3.7. ROSA

5.410 Kubernetes nativo;

5.411 Ser capaz de visualizar todo o fluxo de dados dos PODs no mesmo mapa de fluxo de dados, ou seja, o mapa de fluxo de dados deverá ser único para Servidores, Desktops, Cloud Workload e PODs;

5.412 Ser possível configurar regras de permissão, alerta e bloqueio para comunicações no ambiente. Estas regras deverão também ser baseadas em etiquetas;

5.413 No caso das regras de bloqueio deve minimamente suportar Openshift e Kubernets utilizando CNI OVN ou Calico ou Weve;

5.414 Deverá possuir integração nativa com as plataformas acima para coletar metadados e labels e transformar estes em etiquetas na solução, de forma automática e sem necessidade de ajustes ou customizações na plataforma de Kubernetes e/ou PODs. Deverá ser obrigatoriamente utilizado o objeto “Labels”, não sendo necessário o uso ou criação de qualquer outro objeto no YAML e/ou Kubernetes;

5.415 Deverá também refletir de forma automática, qualquer alteração de metadados e labels do cluster, ajustando as regras de segmentação já criadas;

5.416 Ser capaz de visualizar todo o fluxo de dados dos PODs no mesmo mapa de fluxo de dados, ou seja, o mapa de fluxo de dados deverá ser único para Servidores, Desktops, Cloud Workload e PODs;

5.417 Deverá apresentar informações de comunicação entre os PODs, incluindo qual o processo (container) que originou ou recebeu a comunicação, a porta e o protocolo utilizado, além da imagem e linha de comando utilizada, suportando a identificação de uso indevido dentro da plataforma de kubernetes;

5.418 Deverá apresentar o fluxo de dados leste-oeste e norte-sul (comunicação de e para a internet);

5.419 A instalação do agente deverá ser executada via HELM;

5.420 A solução não deve limitar a quantidade de PODs utilizados por nó de cluster, estando este limitado apenas ao suporte oficial da plataforma de kubernetes;

5.421 A solução não deve gerar nenhum tipo de impacto ou atraso na subida de recursos do ambiente de kubernetes (PODs, Serviços e Etc);

5.422 A solução deve permitir de forma simples criar regras de proteção (bloqueio) e com apenas uma regra bloquear um acesso externo ao cluster acessar uma aplicação interna ao cluster, reduzindo esforço administrativo e dificuldade no entendimento final da regra (Ex.: Block VM Externa -> K8s App);

5.423 VISIBILIDADE

5.424 A solução deverá prover visibilidade de toda a comunicação de rede de forma gráfica, através de um mapa de rede;

5.425 Deve permitir navegar facilmente pelo mapa e focar em parte específica do data center ou aplicativos específicos;

5.426 Deve possuir, no mapa de rede, filtros de inclusão e exclusão, permitindo filtrar no mínimo:

5.427 IP;

5.428 Porta;

5.429 Aplicação, Binário e Serviço;

5.430 Nome do Ativo;

5.431 Tipo de Conexão - Estabelecida, falhada (time out), bloqueada e as que violaram uma política;

5.432 Internet - Com Origem e Destino da Internet;

5.433 Usuário que iniciou o processo;

5.434 Ser possível criar diferentes mapas de rede, determinando o período de tempo e aplicando filtros conforme item anterior;

5.435 Deve ser possível remover Mapas de Fluxo de Dados;

5.436 Deve reter os fluxos de dados por um mínimo de 45 dias, sendo possível criar ou visualizar os mapas utilizando períodos históricos;

5.437 A tela do Mapa de Dados deve possuir mecanismo de busca;

5.438 O mapa de dados deverá apresentar informações de comunicação em Camada 4 e Camada 7;

5.439 Deverá ser possível aplicar Etiquetas diretamente na tela do Mapa de Dados, de forma pontual (único ativo) ou para vários ativos ao mesmo tempo;

5.440 Deverá ser possível verificar as Etiquetas aplicadas a um ativo diretamente da tela do Mapa de Dados;

5.441 Ser possível identificar a quantidade de vezes que uma determinada comunicação aconteceu em um período de tempo;

5.442 Ser possível, no mapa de dados, obter informações do container que efetuou uma determinada comunicação, possuindo no mínimo informações do Caminho do Binário no Ativo, o PID, o HASH, o usuário que executou o processo e a linha de comando executada;

5.443 Deve ser possível, no mapa de dados, visualizar as comunicações de todos os ativos do ambiente, POD a POD;

5.444 Deve ser possível, no mapa de dados, agrupar os ativos através das etiquetas existentes no ambiente, permitindo ainda hierarquizar em subgrupos;

5.445 Deve registrar e apresentar todos os fluxos de comunicação do datacenter, em formato de tabela, juntamente com informações contextuais e detalhadas sobre as cargas de trabalho e aplicativos (container) de comunicação;

5.446 Deve fornecer recursos de filtragem (Ip/Porta/Processo/Origem/Destino/Usuário que iniciou a comunicação) se a comunicação foi estabelecida/bloqueada;

5.447 Deve descobrir automaticamente qualquer novo fluxo de comunicação em tempo real;

5.448 Deve ser possível filtrar os fluxos de dados por um conjunto de regras aplicados no ambiente;

5.449 Deve ser possível exportar os fluxos de dados no mínimo em CSV;

5.450 Deve ser possível visualizar todos os ativos, através da console, obtendo informações da primeira vez que foi visto e a última vez que o ativo se comunicou com a console;

5.451 Deverá ser possível etiquetar ou aplicar TAGs nos ativos do ambiente, ativos com agentes e sem agentes, para utilizar tanto na visualização, em políticas bem como em filtros;

5.452 Não deve existir um limite no tipo e/ou nome de Etiquetas a serem criadas na solução, para as categorias e para os valores;

5.453 Deverá ser possível agrupar etiquetas em Grupos de Etiquetas, para uso nas políticas e outras partes da solução;

5.454 Deverá ser registrado em Log toda a criação, remoção ou modificação das etiquetas, informando no mínimo o usuário responsável, hora e data e a etiqueta alterada. Esses logs deverão ser acessíveis através da própria console de gerenciamento;

5.455 Deverá ser possível aplicar uma etiqueta a um único dispositivo, e também a um conjunto de dispositivos;

5.456 A console de gerenciamento deverá possuir uma área específica de informações dos ativos que devem apresentar todas as Etiquetas aplicadas ao ativo;

5.457 As etiquetas poderão ser utilizadas no Mapa de Visualizações de Fluxo de Dados e nas criações de políticas;

5.458 Deverá apresentar no mapa de fluxo de dados os dispositivos gerenciados e não-gerenciados pela solução;

5.459 MICRO SEGMENTAÇÃO E SEGURANÇA DO AMBIENTE

5.460 Deve fornecer a capacidade de monitorar políticas de tráfego Leste-Oeste e Norte-Sul flexíveis até o nível de uma única carga de trabalho e aplicativo (POD);

5.461 Deve permitir criar e monitorar políticas de comunicação de aplicativo a partir do mapa de visualização;

5.462 Deve suportar regras definidas sobre grupos de ativos de acordo com sua função ou etiquetamento;

5.463 Deve possuir no mínimo 3 (três) tipos de regras: Bloqueio, Permissão e Alerta;

5.464 Deve permitir trabalhar tanto com Whitelist como Blacklist, de forma independente;

5.465 Deve permitir criar regras de micro segmentação utilizando os seguintes parâmetros como Origem e Destino:

5.466 Etiquetas e Grupo de Etiquetas

5.467 IP/Subrede

5.468 Internet (Comunicação vindo da Internet / Rede Interna)

5.469 Qualquer (Any)

5.470 Deve permitir criar regras de Bloqueio, Permissão e Alerta utilizando a Porta e Protocolo (TCP/UDP), incluindo ICMP;

5.471 Deve ser possível criar regras de bloqueio, permissão e alerta, de forma independente. Por exemplo, criar somente uma regra para alertar caso uma aplicação de um namespace se comunique com a aplicação de outro namespace;

5.472 Deve ser possível criar regras somente de bloqueio, sem precisar fazer uma Whitelist da aplicação. Por exemplo, com uma única regra bloquear todos os servidores de Banco de Dados de receber comunicação da Internet;

5.473 Deve ser possível agrupar ou nomear um conjunto de regras com a mesma finalidade, para facilitar o gerenciamento, visualização e filtros por esse agrupamento;

5.474 Ser possível desabilitar uma regra, ou um conjunto de regras, sem a necessidade de excluir da console;

5.475 Possuir filtros de informações no gerenciamento das regras do ambiente;

5.476 Ser possível identificar e filtrar as regras pelo usuário que a criou;

5.477 As regras devem ser publicadas manualmente para os ativos, podendo inclusive escolher se serão aplicadas todas as regras ou um conjunto específico baseado no nome do agrupamento;

5.478 Deve salvar as revisões de política e permitir a reversão para versões anteriores;

5.479 A solução deve possuir nativamente modelos (templates) pré-definidos para aplicações conhecidas de mercado (Ex.: Active Directory), tendo o catálogo disponibilizado na própria console de gerenciamento;

5.480 Deve possuir nativamente modelos (templates) pré-definidos para políticas de Prevenção de Ransomware;

5.481 A solução deve sugerir automaticamente aplicação de políticas de micro segmentação para as aplicações existentes no ambiente;

5.482 Deve sugerir a criação de regras de forma automática com base no fluxo histórico de comunicação das aplicações (mínimo de 30 dias como base de pesquisa);

5.483 Deve poder sugerir políticas automaticamente de acordo com os dados coletados;

5.484 A solução deve utilizar Inteligência Artificial para analisar fluxos de dados históricos (mínimo de 30 dias) e sugerir políticas de segmentação para qualquer aplicação do ambiente;

5.485 Deve ser possível criar políticas com Lógicas de E OU;

5.486 Deve ter a capacidade de isolar uma aplicação, ou um grupo de aplicações, com uma única regra;

5.487 A solução deverá permitir a criação de políticas baseado nos Feeds de Ameaças (Threat Intel) da própria plataforma, possibilitando alertar ou bloquear a comunicação de um Binário, IP ou Domínio malicioso;

5.488 Deve informar ao usuário o impacto das regras criadas no fluxo de comunicação de forma visual, simulando o impacto das regras no fluxo de comunicações;

5.489 Deve detectar, analisar e relatar suspeitas de tentativas de movimento lateral;

5.490 Deve ser capaz de permitir tipos de eventos personalizáveis, prioridade e

gravidade para tipos de eventos individuais;

5.491 Deve permitir editar listas de indicadores confiáveis;

5.492 Deve permitir a definição de políticas de inspeção - tráfego e cargas de trabalho que devem ser completamente ignoradas, bem como tráfego e cargas de trabalho que devem ser ignoradas na investigação de fraude dinâmica de ameaças;

5.493 Deve alertar sobre a violação da política e fornecer informações detalhadas sobre a violação da conexão, indicando inclusive qual container iniciou a comunicação;

5.494 Deve possuir mecanismo de reputação de hash para todo e qualquer processo que tente se comunicar com a rede;

5.495 Deve permitir a integração com fontes externas de informação para aumentar a base de detecção de hashes;

5.496 Deve possuir mecanismo de reputação de DNS e validar toda e qualquer tentativa de resolução de nomes nos ativos protegidos pela solução;

5.497 Deve possuir mecanismo de reputação de IP, para evitar comunicações de IP's sabidos como maliciosos da internet;

5.498 É necessário oferecer a opção de verificar todos os processos de comunicação como parte de malware conhecido por um serviço de reputação incluído;

5.499 INTEGRAÇÕES

5.500 Deve fornecer alertas em tempo real contendo relatórios completos de eventos de segurança;

5.501 Deve suportar a personalização de alertas por gravidade, conteúdo etc;

5.502 Deve poder enviar alertas por email;

5.503 Deve oferecer suporte ao mascaramento de informações confidenciais de alertas por e-mail (ou seja, senhas);

5.504 É necessário integrar-se ao SIEM através de SYSLOG;

5.505 Deve poder enviar alertas e auditar dados para o Slack;

5.506 Deve poder exportar IOCs para o formato STIX;

5.507 Deve suportar uma API para integração personalizável com serviços externos;

5.508 Deve possuir integração com ferramenta de análise de vulnerabilidade, como Tenable, para coletar metadados e criar etiquetas baseada em Vulnerabilidades existentes;

5.509 Possuir integração com F5 BIG-IP;

5.510 Possuir integração com ferramenta de gerência centralizada de Firewalls, como AlgoSec;

5.511 Possuir integração com Firewall Palo Alto, para envio de IPs maliciosos;

5.512 SERVIÇO ESPECIALIZADO PARA INSTALAÇÃO, MIGRAÇÃO E SUPORTE PREVENTIVO/CORRETIVO -24 (VINTE E QUATRO) MESES – GRUPO 2 – ITENS 22 e 23

5.513 Serviço de suporte especializado para instalação, ajustes, configurações e migrações da solução a ser fornecida;

5.514 Além do serviço inicial de instalação e configuração, neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução, seja este corretivo ou preventivo, bem como a transferência de conhecimento hands-on;

5.515 Num prazo de até 10 (dez) dias úteis após a conclusão de instalação da solução ofertada, a contratada deverá fornecer documentação final contendo os manuais de instalação, configurações e utilização. A documentação deverá ser aprovada pela

contratante, caracterizando a conclusão dos serviços;

5.516 Para prestação destes serviços, a CONTRATADA deverá empregar funcionários devidamente qualificados na utilização desse tipo de ferramenta;

5.517 O serviço em questão deve atuar em conjunto com o suporte especializado do fabricante para atuação na manutenção e aplicação das melhores práticas no ambiente;

5.518 A CONTRATADA deverá prover equipe técnica especializada própria para atuar nas demandas da CONTRATANTE durante o contrato vigente;

5.519 **TREINAMENTO OFICIAL – Grupo 2**

5.520 O treinamento deverá iniciar em até 30 dias após a assinatura do contrato;

5.521 Treinamento oficial do fabricante, em modelo presencial ou virtual;

5.522 Deverá ser ministrado em horário comercial;

5.523 Emissão de certificado;

5.524 Carga horária mínima de no mínimo 40 horas;

5.525 Deverá ser ministrado por profissional contratado e certificado pelo fabricante;

5.526 Utilizar como base de elemento prático a solução implantada;

5.527 Utilizar laboratórios práticos virtuais e demonstrações para os casos de soluções ainda não implementadas ou não disponíveis;

5.528 Demonstrar funcionalidades da solução, a fim de capacitar analistas e técnicos que irão atuar na administração, gerenciamento e sustentação da solução;

5.529 Ministrar minimamente os seguintes tópicos:

5.530 Conceitos de microssegmentação;

5.531 Conceitos da solução, arquitetura básica e integrações;

5.532 Arquitetura avançada, gerenciamento e configuração;

5.533 Instalação, configuração e atualização de agentes;

5.534 Criação e manutenção de políticas e regras de detecção;

5.535 Regras de usuários baseado em controle de acesso;

5.536 Detecções e resposta a incidentes;

5.537 Gerenciamento de alertas;

5.538 Monitoramento;

5.539 Investigação de incidentes;

5.540 Laboratórios práticos;

5.541 Num prazo de até 10 (dez) dias úteis, após a conclusão do treinamento, a contratada deverá fornecer documentação dos certificados de cada participante;

5.542 Num prazo de até 5 (cinco) dias úteis, a CONTRATANTE emitirá o Termo de Homologação;

5.543 **EXIGÊNCIAS TÉCNICAS E OPERACIONAIS – Grupo 1 e 2**

5.544 A LICITANTE deverá prever os seguintes Níveis de Serviços para garantia e suporte:

5.545 Plantão técnico de suporte de atendimento: 24 x 7 x 365;

5.546 Plantão técnico de suporte on-site: 24 x 7 x 365;

5.547 Atendimento técnico emergencial local para indisponibilidade dos serviços em até 04 (quatro) horas;

5.548 Atendimento técnico emergencial local para indisponibilidade parcial ou degradação dos tempos de acesso e resposta dos serviços em até 04 (quatro) horas;

5.549 Atendimento técnico para análises, alterações de parâmetros, consulta e suporte geral em até 24 (vinte e quatro) horas.

5.550 A CONTRATADA deverá disponibilizar à CONTRATANTE o serviço de um gestor responsável pelo Contrato de Garantia e Suporte. Este deverá ser o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalonamentos ou problemas de atendimento do Suporte Técnico.

5.551 A LICITANTE não poderá transferir a outrem os compromissos assumidos, no todo ou em parte dos serviços objeto desta contratação.

5.552 Todos os componentes e acessórios deverão ser entregues instalados e funcionando perfeitamente.

5.553 Os serviços de instalação e manutenção não deverão obstruir o andamento das rotinas de trabalho dos ambientes objetos de intervenção. Quando da intervenção nestes ambientes, será de responsabilidade da CONTRATADA, a recomposição total dos mesmos, deixando os locais totalmente limpos e arrumados, inclusive com relação a algum dano a eles causado quando da execução dos serviços.

5.554 Quando da execução dos serviços, os locais de trabalho deverão ser mantidos desobstruídos e bem sinalizados, quando for o caso, de maneira a não comprometer a segurança daqueles que ali trafegam.

5.555 Após a execução dos serviços, as áreas deverão ser mantidas limpas, retirando-se toda e qualquer impureza e sobras de materiais.

5.556 Para facilitar os procedimentos da Secretaria Municipal de Inovação e Tecnologia – SEMIT, a CONTRATADA deverá apresentar planilhas específicas, para cada local que foi objeto de intervenção, constando relação detalhada dos produtos efetivamente instalados, dos desempenhos esperados e especificação dos procedimentos técnicos e, se couber, dos instrumentos usualmente adotados para se efetuar os testes.

5.557 A recusa da aceitação dos serviços deverá ser feita por escrito e conterá os elementos que motivaram a sua determinação. Assim, elencará os produtos ou serviços que estão em desacordo com as especificações e/ou os defeitos apresentados. Diante disso, a CONTRATADA se disporá a consertar, ajustar, substituir os produtos ou fazer os serviços apontados na correspondência da Secretaria Municipal de Inovação e Tecnologia – SEMIT e no término, reapresentará o resultado à SEMIT.

5.558 Fica estabelecido que não ocorrendo nenhum comunicado da Secretaria Municipal de Inovação e Tecnologia – SEMIT, conforme consta no item anterior, os serviços serão considerados automaticamente aceitos. Ressalva-se que fica reservado à SEMIT o direito de exigir, a qualquer tempo, durante a garantia do fornecimento do serviço contratado, a substituição de qualquer acessório, componente ou produto requerido e instalado, que não apresentar as características de desempenho e funcionalidade exigidas, ou venha a apresentar falhas intermitentes não sanadas pela CONTRATADA.

6 ESCOPO DO FORNECIMENTO

6.0 Os fornecimentos deverão prever todos os equipamentos, componentes e subcomponentes, objetivando garantir a total conectividade e interoperabilidade, que deverão resultar no perfeito funcionamento do conjunto, com níveis de desempenho adequados aos fins a que se destinam no contexto de melhorias nos Serviços de TIC da PMS.

6.1 Correrá por conta exclusiva da CONTRATADA a responsabilidade por todas as

despesas de instalação, suporte técnico remoto e local bem como deslocamento dos seus técnicos ao local da instalação e manutenção dos equipamentos, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes.

6.2 Caso a LICITANTE necessite fornecer hardwares e/ou softwares adicionais não especificados nominalmente neste Termo de Referência, mas necessários para atender as funcionalidades exigidas, o custo desses deverão estar inseridos no preço total ofertado.

6.3 Todos os componentes e subcomponentes objetos deste Termo de Referência deverão ser novos, de primeiro uso, sem previsão de descontinuidade anunciada, com tecnologia atualizada e avançada, em linha de produção atendendo às características técnicas presentes nos anexos deste Termo de Referência.

6.4 INSTALAÇÃO, GARANTIA, SUPORTE E TESTES

6.5 O prazo de garantia dos equipamentos e licenciamento da solução é de 24 (vinte e quatro meses);

6.6 Para a garantia, a CONTRATADA deverá observar os procedimentos destinados a recolocar em perfeito estado de operação os serviços tais como:

6.7 No que tange a hardware: instalação, reconfiguração ou reinstalação decorrentes de falhas no hardware ou software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

6.8 No que tange a software: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

6.9 O provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia técnica;

6.10 A CONTRATADA deverá disponibilizar, a instalação da solução, sua garantia do fabricante por 24 (vinte e quatro) meses e prestação dos serviços, incluindo suporte técnico, atendimento on-site e treinamento de acordo com os demais itens deste Termo de Referência, uma equipe com perfil técnico adequado às atividades previstas, com técnicos treinados pelo fabricante para a operação e configuração de todos os componentes ofertados.

6.11 A CONTRATADA deverá apresentar em até 10(dez) dias corridos após a assinatura do contrato reconhecimento do Fabricante, comprovando que a empresa licitante é integradora autorizado e está apto para comercializar, prestar serviços de garantia, instalar, configurar e prestar manutenção para os itens que constituem o objeto desta Licitação

6.12 Os chamados de suporte deverão ser abertos diretamente na contratada, gerenciados pelo mesmo, através de número telefônico 0800 ou equivalente a ligação local e também por ambiente WEB, fornecendo, neste momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos prazos estabelecidos.

6.13 Durante todo o período de garantia contratado, o serviço de suporte deverá ser suprido 24 (vinte e quatro) horas, 07 (sete)dias por semana.

6.14 A CONTRATADA deve disponibilizar acesso ao ambiente WEB do fabricante para download de arquivos e drivers.

6.15 Todo serviço de suporte deverá ser realizado por profissional qualificado;

6.16 O serviço de suporte deverá proporcionar a interação com a equipe técnica da Secretaria Municipal de Inovação e Tecnologia – SEMIT, fornecendo apoio na resolução de incidentes que envolvam os componentes da oferta, garantindo seu pronto reestabelecimento.

6.17 A CONTRATADA manterá registro de todos os chamados abertos, disponibilizando, para cada um, no mínimo as seguintes informações:

6.18 Número sequencial da ordem;

6.19 Data e hora de abertura;

6.20 Severidade;

6.21 Descrição do problema;

6.22 Data e hora do início do atendimento;

6.23 Data e hora de término do atendimento (solução).

6.24 Após o início do atendimento, o tempo de solução do problema deverá ser de acordo com as tabelas abaixo, não devendo ultrapassar os prazos estabelecidos para as respectivas severidades, contados a partir da abertura do chamado técnico;

6.25 Tabela de severidades:

6.26 Severidade

6.27 Descrição

6.28 1 – Crítica O produto não está operante e não é possível nenhuma solução de contorno viável. Problema no produto que gera indisponibilidade em sistemas/serviços

6.29 produtivos que dependem desse ativo.

6.30 2 – Alta Problema no produto que gera impacto em determinado sistema/serviço

6.31 produtivo que dependem desse ativo.

6.32 3 – Média Problema contornável que não gera qualquer impacto aos sistemas/serviços

6.33 produtivos que dependem desses ativos.

6.34 4 – Baixa

6.35 Consultas técnicas e dúvidas sobre os produtos

6.36 Severidade Prazo de atendimento

6.37 TMIA TMSO TMSDC

6.38 1 – Crítica 15 min 6h 48h

6.39 2 – Alta 30 min 8h 72h

6.40 3 – Média 2h 48h 120h

6.41 4 – Baixa 2h 72h 144h

6.42 Entende-se por:

6.43 TMIA - Tempo máximo para início de atendimento: Tempo máximo requerido para o início do atendimento ao produto, que pode ser feito inicialmente por meio telefônico;

6.44 TMSO - Tempo máximo para solução operacional: Tempo máximo de recuperação, ou seja, tempo requerido para contornar o problema e deixar o sistema/serviço disponível;

6.45 TMSDC - Tempo máximo para solução definitiva do chamado: Tempo máximo requerido para solucionar em definitivo a causa do problema.

6.46 Um chamado somente poderá ser fechado após confirmação de responsável do CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

6.47 Este serviço deve estar disponível para acionamento e atendimento no sistema 24x7 (vinte e quatro horas por dia, sete dias na semana);

6.48 Os serviços de manutenção técnica, em atendimento da garantia técnica serão realizados no regime (24x7) vinte e quatro horas por dia, sete dias por semana, respeitando os prazos iniciais da Tabela "Prazo de atendimento"

6.49 O tempo de atendimento será contado a partir do registro do chamado e o de solução será contado a partir do primeiro atendimento.

6.50 Na hipótese de não atendimento aos níveis de serviço especificados, sem prejuízo das sanções administrativas previstas no Regulamento de Licitações e Contratos da Secretaria Municipal de Inovação e Tecnologia – SEMIT, serão aplicados descontos conforme a seguir:

6.51 Descontos por cada hora completa que exceder os níveis de acordo

6.52 Severidade

6.53 0,4% 1

6.54 0,3% 2

6.55 0,2% 3

6.56 0,1% 4

6.57 Os descontos previstos na tabela acima serão calculados tomando como base o valor da garantia contratual e serão descontados dessa garantia prestada pela empresa CONTRATADA;

6.58 O valor do desconto no período será igual ao somatório das ocorrências de não atendimento ou não solução nos níveis de serviço especificados;

6.59 Os descontos aplicados só poderão ser relevados motivadamente e por conveniência administrativa, mediante ato da autoridade competente, devidamente justificado;

6.60 Caso o desconto a ser aplicado seja superior ao valor da garantia, além da perda desta, responderá o contratado pela sua diferença, ou quando for o caso, cobrada judicialmente.

6.61 A garantia deverá ser restabelecida integralmente, caso tenha incidido qualquer desconto sobre o valor desta.

7 LOCAL DE PRESTAÇÃO DOS SERVIÇOS

7.0 Todas as entrega e serviços de instalação e suporte serão executados em qualquer unidade da Prefeitura Municipal do Salvador, conforme orientação da SEMIT.

8 TREINAMENTO

8.0 O Treinamento Oficial elencado na tabela de itens, será efetuado para no mínimo 1 (um) e ou em turmas de 5(cinco) funcionários indicado pelo Gestor do contrato por solução, limitando-se ao total de no máximo 15(quinze) funcionários, atentando-se as especificações técnicas dos treinamentos deste Termo de Referência.

9 OBRIGAÇÕES DA CONTRATADA

9.0 Assegurar a correta integração e funcionalidade dos serviços, em função do projeto e das especificações técnicas constantes neste Termo de Referência.

9.1 Efetuar inspeção/vistoria do local onde ocorrerá a instalação dos equipamentos,

conforme indicação da SEMIT, para verificar os detalhes técnicos de execução.

9.2 Apresentar, ao final do serviço de instalação, o relatório de conclusão do projeto, contendo os seguintes documentos:

9.3 Memorial descritivo de todo o serviço e produtos utilizados;

9.4 Relação de licenças das soluções e serviços.

9.5 Não transferir a outrem, no todo ou em parte, o objeto do presente Termo de Referência, sem prévia e expressa anuência da SEMIT.

9.6 Manter toda estrutura de pessoal e ferramental necessários para execução do contrato, incluindo, fornecimento e serviços, independentemente da demanda definida pela CONTRATANTE.

9.7 Responsabilizar-se por toda a logística (transporte e comunicação) necessária à execução do fornecimento e dos serviços propostos, em todo o Município do Salvador, para atendimento imediato às solicitações da SEMIT, conforme a demanda.

9.8 Arcar com todas as despesas provenientes da limpeza dos locais de instalações e adequações necessárias.

9.9 Manter preposto para representá-la durante a execução dos serviços ora tratados, desde que aceito pela SEMIT.

9.10 Empregar, na execução dos serviços, a equipe técnica indicada na proposta, que poderá ser alterada mediante solicitação de autorização à CONTRATANTE.

9.11 Responder por quaisquer danos que venha a causar à União, Estado, Município ou a terceiros, em função do objeto do contrato firmado, bem como por todos os danos e prejuízos decorrentes de paralisações na execução dos serviços, salvo na ocorrência de motivo de força maior, apurados na forma da legislação vigente, e desde que comunicados à CONTRATANTE no prazo de 48 (quarenta e oito) horas do fato, ou da ordem expressa e escrita da CONTRATANTE.

9.12 Arcar com todas as despesas, diretas ou indiretas, decorrente do cumprimento das obrigações assumidas sem qualquer ônus à CONTRATANTE.

9.13 Arcar integralmente com todas as despesas inerentes à execução dos serviços, tais como, combustíveis, manutenção, seguros, taxas, impostos, tributos e salários.

9.14 Manter, durante toda a execução do Contrato, as mesmas condições da habilitação e qualificação exigidas nesta Licitação.

9.15 Efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente Contrato, bem como observar e respeitar as legislações Federal, Estadual e Municipal relativas ao objeto do Contrato.

9.16 Manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e mão de obra para execução dos serviços.

9.17 Reparar, corrigir, remover, reconstruir ou substituir, total ou parcialmente, às suas expensas, os equipamentos e serviços objeto do fornecimento em que se verifiquem vícios, defeitos ou incorreções, resultantes de execução irregular, do emprego de materiais ou equipamentos inadequados, se for o caso, ou não correspondentes ao serviço.

9.18 Apresentar composição de preços detalhada para aprovação da CONTRATANTE.

9.19 Acatar as normas e condições deste Termo de Referência e seus anexos, independente de transcrição.

9.20 Disponibilizar um profissional que acompanhará as ações junto à SEMIT para

recebimento de Ordens de Serviço, informações, contato com os técnicos responsáveis pelos serviços, coordenação, administração e supervisão do seu pessoal, bem como de qualquer comunicação junto à CONTRATANTE.

9.21 Permitir e facilitar a atuação de auditores e inspetores de qualquer natureza, sempre que necessário.

9.22 Arcar com indenização pecuniária decorrente dos danos morais ou materiais causados por seus empregados em bens patrimoniais da CONTRATANTE, bem como por desaparecimento de quaisquer objetos e valores encontrados em suas dependências, de quem quer que seja, desde que comprovado dolo ou culpa, do empregado da CONTRATADA.

9.23 Afastar ou substituir dentro de 24 (vinte e quatro) horas, sem ônus para a CONTRATANTE, qualquer funcionário que, por solicitação justificada da Fiscalização, não tenha condição de continuar a participar da execução dos serviços.

9.24 Realizar regularmente os exames de saúde dos seus empregados, na forma da lei, assim como arcar com todas as despesas decorrentes de transporte, alimentação, inclusive seguro de vida contra os riscos de acidentes de trabalho e outras especificadas nos dissídios ou convenções coletivas.

9.25 Cada prestador de serviço da contratada deverá apresentar-se uniformizado, com fardamento padrão fornecido pela CONTRATADA, e portando crachá de identificação.

9.26 Manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente do fornecimento e dos serviços objeto deste Contrato.

9.27 Responder perante à CONTRATANTE pela conduta, frequência, pontualidade e assiduidade de seus empregados e efetuar as substituições daqueles que venham a se ausentar do serviço, por motivo justificado ou não, sem nenhum ônus para a CONTRATANTE, bem como comunicar à SEMIT, antecipadamente, todo e qualquer afastamento, substituição ou inclusão de qualquer um dos seus empregados vinculados à execução do presente Contrato.

9.28 Zelar pela boa e completa execução dos serviços e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pela SEMIT, atendendo prontamente às observações e exigências que lhe forem solicitadas.

9.29 Não efetuar despesa, celebrar acordos, fazer declarações ou prestar informações em nome da SEMIT.

9.30 Comunicar imediatamente ocorrências de qualquer natureza que impeçam o bom andamento do serviço.

10 OBRIGAÇÕES DA CONTRATANTE

10.0 Proporcionar à CONTRATADA todas as facilidades para que possa desempenhar o objeto da Licitação de forma satisfatória.

10.1 Designar uma equipe técnica para fiscalizar e acompanhar a execução do fornecimento e serviços prestados.

10.2 Promover o acesso às unidades dos órgãos e entidades da PMS das equipes da CONTRATADA que executarão a entrega e os serviços de instalação e suporte.

10.3 Prestar as informações e os esclarecimentos que venham a ser solicitados pelos responsáveis da CONTRATADA.

10.4 Dar ciência à CONTRATADA de quaisquer modificações que venham a ocorrer.

10.5 Atestar as notas fiscais/faturas, por servidor/comissão competente, emitidas pela

CONTRATADA, recusando-as quando inexatas ou incorretas, efetuando todos os pagamentos nas condições pactuadas.

10.6 FISCALIZAÇÃO

10.7 A SEMIT fica investida dos mais amplos poderes para fiscalizar toda a execução do objeto, impugnando quaisquer erros ou omissões que considere em desacordo com as obrigações da CONTRATADA.

10.8 PAGAMENTOS

10.9 O pagamento será realizado pela contratante, através de crédito em conta corrente, obrigatoriamente mantida junto ao Banco Bradesco, consoante determinação do Decreto Municipal n.º 23.856/2013 (arts. 1º a 4º), com observância das exceções ali previstas (art. 5º, parágrafo único), a qual deverá ser indicada na declaração fornecida pelo estabelecimento bancário, na forma do disposto no art. 4º, § 2º do Decreto Municipal 13.991/2002, no prazo de até 20 (vinte) dias úteis, contados da apresentação da Nota Fiscal/Fatura, em conformidade com a legislação vigente, mediante a apresentação dos documentos fiscais exigíveis e declaração de não existência de débitos registrados no CADIN Municipal, conforme Decreto Municipal nº 24.419/2013.

10.10 As notas fiscais/faturas somente deverão ser apresentadas para pagamento após a entrega dos materiais e serviços, sendo que o prazo para pagamento somente fluirá após o efetivo atesto do recebimento definitivo.

10.11 Na ocorrência de necessidade de providências complementares por parte da contratada, o decurso do prazo de pagamento será interrompido, reiniciando-se sua contagem a partir da data em que estas forem cumpridas, caso em que não será devida nenhuma atualização financeira.

10.12 Nenhum pagamento será efetuado à contratada enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito a reajustamento de preço ou correção monetária.

11 VISTORIA TÉCNICA

11.0 Fica facultado à LICITANTE interessada, realizar vistoria técnica no DATACENTER da SEMIT/COGEL para tirar todas as dúvidas e tomar conhecimento pleno das condições ambientais e técnicas para a efetiva realização da entrega do solicitado. Não serão aceitas alegações posteriores de desconhecimento das condições necessárias e requerimentos de compatibilidade à execução dos serviços. Caso seja de interesse da LICITANTE, a vistoria técnica deverá ser agendada pelo telefone (71) 3202-4295 na pessoa do Raphael da Fonseca Monteio, até 72 (setenta e duas) horas antes da data do certame.

11.1 A comprovação da visitação será feita através da emissão, pela SEMIT, de Declaração de Vistoria Técnica.

12 HABILITAÇÃO TÉCNICA

12.0 A empresa Licitante deverá apresentar atestado(s) de Capacidade Técnica, expedido(s) por pessoa jurídica de direito público ou privado, comprovando aptidão para a execução que a mesma tenha executado serviço semelhante e compatível com solução de cibersegurança com visibilidade e proteção de ameaças na rede.

12.1 Os atestados deverão ser impressos em papel timbrado, com nome e telefone de contato dos responsáveis pela informação atestada, não sendo aceitas declarações genéricas, devendo ainda atestar a satisfação com o serviço ofertado pela PROPONENTE.

12.2 A CONTRATANTE se reserva o direito de conferir as informações prestadas pelas

empresas emitentes dos atestados, através de consultas e visitas, bem como a disponibilidade de equipamentos solicitados junto à PROPONENTE.

12.3 A PROPONENTE deverá apresentar os seguintes documentos:

12.4 Indicação de site na WEB para transferência de arquivos de configuração (manuais e atualizações de firmware);

12.5 Prospecto com as características técnicas de todos os componentes dos equipamentos, incluindo especificação de marca, modelo e outros elementos que, de forma inequívoca, identifiquem e comprovem as configurações cotadas, possíveis expansões e upgrades, através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em websites dos fabricantes na Internet, em que conste o respectivo endereço eletrônico;

12.6 Deve ser apresentada uma planilha de comprovação técnica para todas as especificações exigidas neste termo de referência através de documento oficial do fabricante, pagina e texto de comprovação.

12.7 Indicação exata do modelo de equipamento ofertado, no Sistema Eletrônico de Disputas e na Proposta de Preços, sendo os respectivos catálogos obrigatoriamente de domínio público, ou seja, deverão estar publicados no website do fabricante, comprovando todos os recursos e funcionalidades mínimas exigidas para os equipamentos que irão integrar as características técnicas solicitadas no Anexo A.

12.8 O não cumprimento dos quaisquer dos requisitos de habilitação, ensejará na automática inabilitação da proponente.

13 SIGILO DE INFORMAÇÕES CADASTRAIS

13.0 Todas as informações relativas à CONTRATANTE e constantes do cadastro da CONTRATADA deverão ser tratadas como confidenciais e somente poderão ser fornecidas quando solicitadas:

13.1 Pela CONTRATANTE;

13.2 Em decorrência de determinação judicial.

13.3 Os conhecimentos, dados e informações de propriedade do Município, relativos a aspectos econômico-financeiros, tecnológicos e administrativos, tais como produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do presente Termo de Referência, constituem informação privilegiada e como tal, tem caráter de confidencialidade, só podendo ser utilizados, exclusivamente, no cumprimento e execução das condições estabelecidas neste Contrato, sendo expressamente vedado à CONTRATADA:

13.4 Utilizá-los para fins outros, não previstos neste Instrumento;

13.5 Repassá-los a terceiros e empregados não vinculados diretamente ao objeto proposto.

14 PRAZO DE ENTREGA DOS SERVIÇOS E MATERIAIS

14.0 A CONTRATADA deverá realizar a entrega, instalação e todas as configurações dos equipamentos em até 60 (sessenta) dias, contados da data de assinatura do Contrato, iniciando neste momento a prestação dos serviços objetos desta contratação.

14.1 Os serviços terão seus prazos estipulados nas Ordens de Serviços (OS) emitidas pela SEMIT, durante o período de validade estabelecido pelo Contrato, com vigência de 24 (vinte e quatro) meses, podendo ser prorrogado mediante termo aditivo, devidamente justificada a conveniência na forma permitida em lei.

14.2 Justifica-se este prazo de vigência devido à necessidade de preparação de

estrutura física e técnica que devem ser implantados para o correto funcionamento das soluções de segurança, garantindo exequibilidade ao contrato em função da diluição do investimento em um prazo mais estendido. Caso fosse estabelecido prazo menor, acarretaria um maior custo para administração, considerando ainda que as cotações constantes na pesquisa de preço foram realizadas com previsão de contratação de 24 meses, o que exigiria a realização de nova pesquisa. Além disso, por ser um serviço essencial por se tratar da segurança da informação a Prefeitura de Salvador não pode incorrer no risco de interromper o serviço em um prazo menor que o estipulado em contrato.

14.3 A CONTRATADA Será responsável pela Garantia e Suporte técnico por 24 (vinte e quatro) meses, contados da implantação da solução.

15 CONDIÇÕES GERAIS

15.0 O atendimento para executar o fornecimento e os serviços se dará mediante emissão do contrato/empenho datada e assinada pela Unidade demandante.

15.1 Atesto, para os devidos fins licitatórios, que as especificações técnicas aqui contidas neste Termo de Referência se encontram em consonância com as disposições legais e normativas aplicáveis e com interesse e conveniência da Administração, afastando-se as características, cláusulas e condições que direcionem, comprometam, restrinjam ou frustrem o caráter competitivo da Licitação.

15.2 Afiança-se, ainda, que as especificações técnicas fornecidas são suficientes para elaboração das propostas pelos interessados em contratar com a Administração Municipal.

15.3 Declaro que não existem, neste Termo de Referência e seus anexos, especificações que, por excessivas, irrelevantes ou desnecessárias, limitem ou frustrem a competição ou realização do fornecimento (art. 7º, inciso I, Lei Municipal nº 6.148/02; art. 3º, inciso II, Lei Federal nº 10.520/02; art. 3º, § 1º, inciso I, Lei Federal nº 8.666/93).

15.4 A SEMIT atesta, para os devidos fins licitatórios, que as especificações técnicas contidas neste Termo de Referência não restringem a competitividade, conforme os pressupostos legais.

15.5 As especificações técnicas das soluções e serviços a serem prestados encontram-se detalhadas no Anexo A.

15.6 O vencedor da Licitação será a empresa que apresentar a proposta com o menor valor global por lote conforme a planilha constante do Anexo B.

15.7 As propostas de preço deverão ser suportadas de informações e documentações detalhadas.

15.8 Todas as informações relativas à CONTRATANTE e constantes do cadastro da CONTRATADA deverão ser tratadas como confidenciais e somente poderão ser fornecidas quando solicitadas.

15.9 Os conhecimentos, dados e informações de propriedade do Município do Salvador, relativos a aspectos econômico-financeiros, tecnológicos e administrativos, tais como produtos, sistemas, técnicas, estratégias, métodos e de operação e todos e quaisquer outros, repassados por força do objeto do presente Termo de Referência e seus Anexos, constituem informação privilegiada e como tal, tem caráter de confidencialidade, só podendo ser utilizados, exclusivamente, no cumprimento e execução das condições estabelecidas neste Documento, sendo expressamente vedado à CONTRATANTE.

16 CONDIÇÕES DA ATA DE REGISTRO DE PREÇOS

16.0 As quantidades estabelecidas para cada um dos itens são estimativas e não constituem compromisso de demanda por parte da Secretaria Municipal de Inovação e

Tecnologia – SEMIT;

16.1 A existência de preços registrados não obriga a Secretaria Municipal de Inovação e Tecnologia – SEMIT a firmar as contratações que deles poderão advir, ficando lhe facultada a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurada ao beneficiário do registro a preferência em igualdade de condições;

16.2 A Secretaria Municipal de Inovação e Tecnologia – SEMIT faculta aos órgãos e entidades da Administração Pública a adesão à ata de Registro de Preços por ela firmada, disponibilizando no instrumento convocatório da licitação como anexos, minutas de contratos destinados ao atendimento das demandas da companhia, bem como para atendimento dos órgãos não participantes;

16.3 Com base no Decreto Federal nº xxxxxxxx, as aquisições ou as contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão ou a entidade gerenciadora e para os órgãos ou as entidades participantes;

16.4 O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão ou a entidade gerenciadora e os órgãos ou as entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

16.5 Os Órgãos e Entidades da Administração Pública, que não participaram do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar a Secretaria Municipal de Inovação e Tecnologia – SEMIT.

16.6 Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente da adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com a Secretaria Municipal de Inovação e Tecnologia – SEMIT;

16.7 Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências à Secretaria Municipal de Inovação e Tecnologia – SEMIT;

16.8 O prazo de validade da ata de registro de preços será de 12 (doze) meses, podendo ser prorrogada por mais 12 (doze) meses a contar da data de sua assinatura.

17 VIGÊNCIA CONTRATUAL

17.0 O prazo de vigência do contrato, a contar da data da sua assinatura, é de 24 (vinte e quatro) meses, podendo ser prorrogado, a critério da CONTRATANTE, conforme previsto no Regulamento de Licitações e Contratos da Secretaria Municipal de Inovação e Tecnologia – SEMIT.

18 OBRIGAÇÕES DA CONTRATADA

18.0 Zelar pelo cumprimento do objeto e das demais cláusulas deste previstas no Termo de Referência e Contrato;

18.1 Prestar os serviços objeto deste Termo de Referência com qualidade, eficiência, presteza, pontualidade e de forma ininterrupta, em conformidade com os termos e prazos estabelecidos;

18.2 Atender às solicitações de serviços de acordo com as especificações técnicas, cronogramas e condições especificadas;

18.3 Prestar os serviços com pessoal adequadamente capacitado em locais e

instalações de acordo com as orientações constantes neste TR;

18.4 Dispor de pessoal necessário para garantir a execução dos serviços, nos regimes contratados, sem interrupção seja por motivo de férias, descanso semanal, licença, falta ao serviço, greve, demissão e outros análogos, obedecidas às disposições da legislação trabalhista vigente;

18.5 Não veicular publicidade ou qualquer outra informação acerca das atividades objeto deste contrato, sem prévia autorização do CONTRATANTE;

18.6 Manter, durante a vigência do contrato, todas as condições de habilitação e qualificação exigidas neste TR;

18.7 Assumir todas as providências e obrigações estabelecidas nas normas de segurança e legislação específica de acidentes de trabalho quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles;

18.8 Assumir todas as despesas e ônus relativos ao seu pessoal, ficando ainda, para todos os efeitos legais, expressos pela CONTRATADA, a inexistência de qualquer vínculo empregatício entre seus empregados e/ou prepostos do CONTRATANTE;

18.9 Acompanhar o cumprimento dos serviços cabendo-lhe integralmente o ônus decorrente de fiscalizá-los, não se eximindo das suas obrigações, independentemente das ações de fiscalização exercidas pelo CONTRATANTE;

18.10 Dar ciência CONTRATANTE, imediatamente e por escrito, de qualquer anormalidade identificada na execução dos serviços, bem como as providências tomadas para a sua solução;

18.11 Assumir total responsabilidade pelo sigilo das informações, dados, contidos em quaisquer mídias e documentos que seus empregados ou prepostos vierem a obter em função dos serviços prestados, mesmo após o término do prazo de vigência ou eventual rescisão do Contrato, respondendo pelos danos que eventual vazamento de informação, decorrentes de ação danosa ou culposa, nas formas de negligência, imprudência ou imperícia, venha a ocasionar ao CONTRATANTE ou a terceiros;

18.12 Responsabilizar-se pelo perfeito funcionamento do objeto do contrato, arcar com os eventuais prejuízos causados ao CONTRATANTE e/ou a terceiros, provocados por ineficiência ou irregularidade cometida por seus empregados ou prepostos envolvidos na execução dos serviços, respondendo integralmente pelo ônus decorrente de sua culpa ou dolo na entrega dos serviços, o que não exclui nem diminui a responsabilidade pelos danos que se constatarem, independentemente do controle e fiscalização exercidos pelo CONTRATANTE;

18.13 Reparar, exclusivamente às suas custas, todos os defeitos, erros, falhas, omissões e quaisquer irregularidades verificadas na oferta de serviços, bem como responsabilizar-se por qualquer dano ou prejuízo daí decorrente;

18.14 Garantir o atendimento dos prazos previstos nos Acordos de Nível de Serviço, sem prejuízo aos demais serviços, sempre que houver a necessidade de execução de correções em serviços já entregues;

19 OBRIGAÇÕES DO CONTRATANTE

19.0 Fiscalizar o cumprimento do objeto e das demais cláusulas deste Termo de Referência e seus anexos;

19.1 Proporcionar as condições necessárias para que a CONTRATADA possa cumprir o que estabelece este Termo de Referência e seus anexos;

19.2 Designar pessoas para os papéis descritos quanto à fiscalização e gestão do

contrato;

19.3 Convocar, realizar e registrar reuniões junto à CONTRATADA;

19.4 Verificar a execução dos serviços;

19.5 Notificar formalmente a CONTRATADA quanto a defeitos ou irregularidades observadas na execução dos serviços e sobre a aplicação de penalidades, assegurada sua prévia defesa;

19.6 Efetuar os pagamentos devidos à CONTRATADA no prazo e nas condições indicadas neste instrumento, desde que atenda as formalidades necessárias, e após aceitação dos serviços pelos meios convencionados;

19.7 Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos profissionais da CONTRATADA ou o seu Preposto;

19.8 Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA, conforme determina a Lei, antes de efetuar o pagamento devido;

19.9 Comunicar à CONTRATADA a necessidade de substituição de qualquer profissional que seja considerado inadequado para o exercício da função.

20 ELEMENTOS NECESSÁRIOS À GESTÃO DO CONTRATO

20.0 Por tratar-se de Registo de Preços, o Gestor e o Fiscal de cada contrato serão indicados no momento da contratação.

21 FORMA DE COMUNICAÇÃO

21.0 A tramitação de documentos entre o CONTRATANTE e a CONTRATADA deverá ser rigorosamente controlada através de documentos protocolados fisicamente ou enviados através de meio eletrônico.

22 SANÇÕES ADMINISTRATIVAS

22.0 Serão aplicadas sanções administrativas ao Licitante que cometer qualquer prática considerada ilícita conforme exposto no Regulamento de Licitações e Contratos da Secretaria Municipal de Inovação e Tecnologia – SEMIT, podendo incidir, em caso de descumprimento contratual, multas ou descontos, bem como, em casos mais graves, rescisão do mesmo.

22.1 No caso de descumprimento total da obrigação principal, será aplicada multa compensatória no percentual de 0,5% (cinco décimos por cento) incidente sobre o valor global do contrato.

22.2 Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicada multa compensatória no percentual de 20% (vinte por cento) incidente sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do serviço já realizado.

22.3 No caso de descumprimento da obrigação acessória, será aplicada multa compensatória no percentual de 5% (cinco por cento) incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada do seu custo.

22.4 No caso de recusa injustificada do adjudicatário em assinar o termo de contrato, em aceitar ou retirar o instrumento equivalente, ou, quando for o caso, em assinar a ata de registro de preços, ou praticar condutas a elas equiparadas, será aplicada multa compensatória no percentual de 5% (cinco por cento) incidente sobre o valor correspondente ao objeto adjudicado ou, quando for o caso, da estimativa da contratação.

22.5 O atraso injustificado na execução do Contrato ensejará a aplicação de multa moratória no percentual de 0,1% (um décimo por cento) ao dia, incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada do seu custo, observado o percentual

máximo total de 30% (trinta por cento).

22.6 O atraso injustificado do prazo fixado para apresentação, suplementação ou reposição de garantia contratual ensejará a aplicação de multa moratória no percentual de 0,1% (um décimo por cento) ao dia, incidente sobre o valor global do contrato.

22.7 A aplicação de multa de mora não impedirá que a Secretaria Municipal de Inovação e Tecnologia – SEMIT a converta em compensatória e promova a extinção unilateral do Contrato com a aplicação cumulada de outras sanções.

22.8 Na hipótese do subitem anterior, se o cálculo da multa moratória atingir o patamar correspondente ao valor máximo da multa compensatória, o recebimento do objeto deverá ser recusado, salvo justificativa escrita devidamente fundamentada, sem prejuízo da aplicação das demais sanções.

22.9 TERMO DE COMPROMISSO E DE CONFIDENCIALIDADE

22.10 A CONTRATADA compromete-se a cumprir e obedecer à Política de Segurança da Informação da Secretaria Municipal de Inovação e Tecnologia – SEMIT.

22.11 A CONTRATADA deverá assinar Termo de Compromisso, Sigilo e Confidencialidade, constante no Anexo I deste Termo, no momento da assinatura do contrato.

23 GARANTIA CONTRATUAL

23.0 A empresa vencedora do certame deverá prestar garantia de 5% (cinco por cento) do valor do contrato, podendo optar por uma das modalidades previstas no Regulamento de Licitações e Contratos da Secretaria Municipal de Inovação e Tecnologia – SEMIT, ficando esclarecido que a garantia deverá ter seu valor atualizado nas mesmas condições do contrato e renovada, quando for o caso, conforme previsto neste Termo de Referência.

24 PARTICIPAÇÃO DE CONSÓRCIOS

24.1. Não será permitida a participação de empresas reunidas em consórcio, considerando a natureza integrada, crítica e sensível do objeto, que envolve solução de cibersegurança para servidores, estações de trabalho, sensores de rede, gerenciamento da superfície de risco, microsegmentação de aplicações, visibilidade de conexões, contenção de rede, instalação, configuração, suporte técnico 24x7, atualização tecnológica e treinamento, conforme especificações constantes deste Termo de Referência.

24.2. A vedação à participação em consórcio justifica-se pela necessidade de preservação da unidade de responsabilidade técnica, operacional, contratual e de segurança da informação, uma vez que a execução do objeto exige integração entre componentes, correlação de eventos, gestão centralizada, resposta a incidentes, tratamento de dados sensíveis, acesso a ambientes críticos e observância de requisitos de sigilo e confidencialidade.

24.3. A admissão de consórcios, neste caso, poderia ampliar a complexidade de gestão contratual, dificultar a identificação objetiva de responsabilidades em caso de falhas, atrasos, incidentes de segurança, indisponibilidade, incompatibilidades técnicas, vazamento de informações ou descumprimento de níveis de serviço, especialmente por se tratar de solução essencial à proteção da infraestrutura tecnológica da Prefeitura Municipal do Salvador.

24.4. A restrição não compromete a competitividade do certame, pois o objeto poderá ser executado por empresas especializadas do mercado de tecnologia e cibersegurança, inclusive fabricantes, representantes, revendas autorizadas ou integradores habilitados, desde que atendam integralmente às condições de habilitação, qualificação técnica, suporte, garantia, sigilo, segurança e demais exigências previstas neste Termo de Referência e no edital.

24.5. Dessa forma, a vedação à participação de consórcios mostra-se adequada, proporcional e compatível com o interesse público, visando garantir maior segurança jurídica, rastreabilidade de responsabilidades, eficiência na fiscalização contratual, continuidade operacional e mitigação de riscos técnicos e administrativos na execução do objeto.

25 PROVA DE CONCEITO (POC)

25.0 Não será exigida prova de conceito, tendo em vista que os requisitos técnicos do objeto são plenamente verificáveis por meio da documentação apresentada na fase de habilitação e julgamento das propostas.

ANEXO I - TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado a Secretaria Municipal de Inovação e Tecnologia – SEMIT , CNPJ nº 13.928.801/0035-98, situada na cidade de Salvador, endereço Rua Miguel Calmon, nº 15, Edf. Sintral Comércio, Salvador-BA, doravante denominada CONTRATANTE, e de outro lado _____, CNPJ nº _____/____, situada na cidade de _____, à Rua: _____, bairro _____, doravante denominada CONTRATADA, têm entre si justa e acertada, a celebração do presente TERMO DE SIGILO E CONFIDENCIALIDADE, através do qual a CONTRATADA aceita não divulgar sem autorização prévia e formal segredos e informações sensíveis de propriedade da Secretaria Municipal de Inovação e Tecnologia – SEMIT e de seus clientes e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

PRIMEIRA – A CONTRATADA reconhece que em razão das suas atividades profissionais, estabelece contato com informações sigilosas, que devem ser entendidas como segredo. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios Colaboradores da CONTRATADA, sem a expressa e escrita autorização da CONTRATANTE;

SEGUNDA - As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito da Secretaria Municipal de Inovação e Tecnologia – SEMIT , transmitidas por meios escritos, eletrônicos, verbais ou quaisquer outros, e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

1.Toda informação relacionada a computador e componentes de software em geral, programas existentes (código fonte/código objeto), ou em fase de desenvolvimento no âmbito da empresa, inclusive fluxogramas, listagens, documentação, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados e versões “beta” de quaisquer programas e rotinas;

2.Documentos, informações e dados armazenados de atuação consultiva e contenciosa, de estratégias ou demais dados e/ou informações de caráter sigiloso ou restrito;

3.Informações e documentos relativos às estratégias de marketing, de negócios, de clientes e os seus respectivos dados, pesquisas de mercado, armazenados sob qualquer forma;

4.Informações de projetos, metodologias, ferramentas de desenvolvimento de aplicativos e serviços desenvolvidos pela Secretaria Municipal de Inovação e Tecnologia – SEMIT ;

5.Números e valores financeiros da empresa tais como: inadimplência, relação de salários, fluxo de caixa, informações de custos, dentre outros;

6.Informações referentes a dados pessoais e/ou dados pessoais sensíveis;

TERCEIRA – A CONTRATADA reconhece que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade que já existam ou que venham a surgir no futuro devem ser mantidas sob segredo. Em caso de dúvida acerca da confidencialidade de determinada informação a CONTRATADA deve tratar a mesma sob sigilo até que seja autorizado, formalmente, a tratá-la de forma diferente pela CONTRATANTE. Em hipótese alguma a CONTRATADA deve interpretar o silêncio da Empresa como liberação de quaisquer dos compromissos ora assumidos;

QUARTA - A CONTRATADA está ciente de que o serviço de correio eletrônico corporativo, caso seja fornecido pela CONTRATANTE para o exercício das atividades, é exclusivo para assuntos pertinentes ao objeto do contrato e reconhece que a CONTRATANTE

tem pleno acesso à essas contas corporativas para quaisquer fins, tais como: auditoria, encaminhamento de assuntos pendentes, configuração de resposta automática, redirecionamento e recuperação de e-mails;

QUINTA – A CONTRATADA reconhece que, ao término do presente contrato _____, deverá entregar à CONTRATANTE todo e qualquer material de propriedade desta, inclusive notas pessoais envolvendo matérias sigilosas relacionadas com a _____, registros de documentos de qualquer natureza que tenham sido usados, criados ou estado sob seu controle. A CONTRATADA também assume o compromisso de não utilizar qualquer informação adquirida quando de suas atividades para a CONTRATANTE;

SEXTA – A CONTRATADA deve assegurar que todos os seus colaboradores guardarão sigilo sobre as informações que porventura tiverem acesso, e que os mesmos se comprometem a informar imediatamente ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional;

Parágrafo Primeiro: A apresentação dos Termos de Sigilo e Confidencialidade de seus colaboradores não exime a CONTRATADA das penalidades por violação das regras por parte destes;

Parágrafo segundo: A CONTRATADA deverá fornecer cópia de todos os termos firmados com seus colaboradores à CONTRATANTE no prazo de 10 (dez) dias após assinatura dos respectivos termos;

Parágrafo Terceiro: Sempre que um colaborador for admitido, A CONTRATADA deverá fornecer cópia dos novos termos firmados no prazo de 2 (dois) dias após assinatura dos respectivos termos;

SÉTIMA - O atendimento deste Termo de Sigilo e Confidencialidade bem como da das Diretrizes Básicas da Política de Segurança da Informação devem ser incorporados formalmente ao contrato de trabalho dos funcionários da CONTRATADA que prestarem serviços à CONTRATANTE;

OITAVA – A CONTRATADA deverá atender às diretrizes estabelecidas na Política de Segurança da Informação definida pela CONTRATANTE;

NONA - A CONTRATADA declara, por fim, que as obrigações a que alude este Termo perdurarão após o término do contrato AA/NNNN-00, e abrangem, além das informações de que venha a tomar conhecimento, aquelas que já possui na presente data;

DÉCIMA - O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização civil e criminal, de acordo com a legislação vigente;

Salvador – BA,_____de _____de 2026.

_____ _____

Responsável pelo Contrato – CONTRATANTE Responsável pelo Contrato – CONTRATA

ANEXO II - MODELO DE PROPOSTA

LOTE ÚNICO
Grupo 1 – Solução de Cybersegurança para Servidores, Estações de Trabalho com Gerenciamento da Superfície

de Risco					
Item	**Descrição**	**Métrica**	**QTD**	**Valor unitário**	**Sub total**
1.	Trend Micro Vision One Endpoint Security Pro, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	1.500		
2.	Trend Micro Email and Collaboration Security, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	34.000		
3.	Trend Micro Deep Discovery Inspector – 4Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	4		
4.	Trend Micro TippingPoint Threat Protection System (TPS) 5Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	4		
5.	Trend Micro TippingPoint Threat Protection System (TPS) 10Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	3		
6.	Trend Micro Plataforma TrendAi Vision One por 24 (vinte e quatro) meses	Unidade	500.000		
7.	Trend Micro Service One Complete (rede 4Gbps), por 24 (vinte e quatro) meses	Unidade	4		
8.	Trend Micro Service One Complete (endpoint) por 24 (vinte e quatro) meses	Unidade	1.500		
9.	Network Packet Broker, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	2		
10.	Módulo mini-gbic SFP+ gigabit Ethernet Base-SR, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	40		
11.	Módulo mini-gbic SFP gigabit Ethernet 10GBASE-T, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	24		
12.	Funcionalidade de Descriptografia de Rede SSL/TLS em linha, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	2		
13.	Funcionalidade de Otimização de Cópia de Tráfego para Ferramentas, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	2		
14.	Gerência Centralizada - Network Packet Broker, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	1		
15.	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 01	Unidade	1.500		
16.	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 02	Unidade	34.000		
17.	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 03	Unidade	4		
1	Serviço especializado para instalação, migração	Unidade	4		

8.	e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 04				
9.	1 Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 05	Unidade	3		
0.	2 Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 09	Unidade	2		
1.	2 Treinamento oficial	Unidade	15		
	A = Valor Total Grupo 1				

Grupo 2 – Solução de Cybersegurança para Microsegmentação de Aplicações com Visibilidade de Conexões e Contenção da Rede					
22.	Solução de microssegmentação, visibilidade e proteção de Rede, baseada em Software, para controle de movimentação lateral em ambiente corporativo de servidores, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	1.500		
23.	Solução de microssegmentação, visibilidade e proteção de Rede, baseada em Software, para controle de movimentação lateral em ambiente corporativos em Containers, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	50		
24.	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 22	Unidade	1.500		
25.	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 23	Unidade	50		
26.	Treinamento oficial	Serviço	15		
	B = Valor Total Grupo 2				
	A + B= VALOR TOTAL (Grupo 1 e 2)				

EDITAL DE PREGÃO ELETRÔNICO – SEMIT Nº 003/2026
ANEXO III
MINUTA DE TERMO DE COMPROMISSO DE FORNECIMENTO Nº. XXX/2026

EDITAL DE LICITAÇÃO PREGÃO Nº. 003/2026 - SEMIT PROCESSO ADMINISTRATIVO Nº. 13202/2026

NOME DO PROMITENTE FORNECEDOR, ENDEREÇO, CNPJ/MF sob o nº _____ através do seu representante legal, _____, R.G. nº _____ CPF nº _____, conforme instrumento em anexo, vem pelo presente TERMO DE COMPROMISSO, firmado com o MUNICÍPIO DO SALVADOR, através da Secretaria Municipal de Inovação e Tecnologia, CNPJ/MF sob o nº 13.927.801/0035-98, neste ato representada pelo Sr. Secretário Municipal ALBERTO VIANNA BRAGA NETO, nos termos do artigo art. 40, inc. II, 78, IV, e 82 e 87 da Lei 14.133/2021 e das demais normas legais aplicáveis, em face da classificação das propostas apresentadas no Pregão Eletrônico do SISTEMA DE REGISTRO DE PREÇOS Nº. XXX/2026, RESOLVE registrar os valores oferecidos, pelo período de 12 meses, conforme consta no Edital do Pregão Eletrônico, que passa a fazer parte desta Ata, tendo sido, os referidos valores, oferecidos pelas empresas cujas propostas foram classificadas no certame.

CLÁUSULA I – DO OBJETO

1.1 Contratação através de sistema de registro de preços objetivando a formalização de ATA com o vencedor do certame, visando a contratação de Solução de Cybersegurança para servidores, estações de trabalho e demais sensores de rede com gerenciamento da superfície de risco e microsegmentação de aplicações com visibilidade de conexões e contenção da rede, para a infraestrutura da SEMIT, na modalidade de subscrição de licença, incluindo suporte técnico no regime 24x7 (vinte e quatro horas por dia, sete dias por semana) e garantia de atualização das versões pelo período de 24 meses, contemplando também, instalação, configuração e treinamento de acordo com as especificações técnicas mínimas e detalhamentos consignados neste Termo de Referência (TR) e seus anexos, com a conveniência e necessidade da Prefeitura Municipal de Salvador – PMS, conforme as especificações, quantitativas e qualitativas e todas as demais condições gerais discorridas neste Termo de Referência (TR).

CLÁUSULA II – DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1 O valor do presente Termo de Compromisso de Fornecimento é o valor ofertado pelo PROMITENTE FORNECEDOR para o(s) lote(s) __, constante(s) de sua proposta, apresentada no Pregão Eletrônico nº ____/2026, que faz parte integrante deste instrumento, independentemente de transcrição, perfazendo o valor total de R$ _____(_____), fixo e só reajustável na forma da lei.

LOTE ÚNICO

Grupo 1 – Solução de Cybersegurança para Servidores, Estações de Trabalho com Gerenciamento da Superfície de Risco					
Item	**Descrição**	**Métrica**	**QTD**	**Valor unitário**	**Subtotal**
1.	Trend Micro Vision One Endpoint Security Pro, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	1.500		
2.	Trend Micro Email and Collaboration Security, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	34.000		
3.	Trend Micro Deep Discovery Inspector – 4Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	4		
4.	Trend Micro TippingPoint Threat Protection System (TPS) 5Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	4		
5.	Trend Micro TippingPoint Threat Protection System (TPS) 10Gbps, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	3		
6.	Trend Micro Plataforma TrendAi Vision One por 24 (vinte e quatro) meses	Unidade	50.000		
7.	Trend Micro Service One Complete (rede 4Gbps), por 24 (vinte e quatro) meses	Unidade	4		
8.	Trend Micro Service One Complete (endpoint) por 24 (vinte e quatro) meses	Unidade	1.500		
9.	Network Packet Broker, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	2		
10.	Módulo mini-gbic SFP+ gigabit Ethernet Base-SR, incluindo garantia e atualização de versão por 24 (vinte e quatro)	Unidade	40		

	meses				
1. 1	Módulo mini-gbic SFP gigabit Ethernet 10GBASE-T, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	24		
2. 1	Funcionalidade de Descriptografia de Rede SSL/TLS em linha, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	2		
3. 1	Funcionalidade de Otimização de Cópia de Tráfego para Ferramentas, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	2		
4. 1	Gerência Centralizada - Network Packet Broker, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	1		
5. 1	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 01	Unidade	1.500		
6. 1	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 02	Unidade	34.000		
7. 1	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 03	Unidade	4		
8. 1	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 04	Unidade	4		
9. 1	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 05	Unidade	3		

20.	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 09	Unidade	2		
21.	Treinamento oficial	Unidade	15		
	A = Valor Total Grupo 1				
Grupo 2 – Solução de Cybersegurança para Microsegmentação de Aplicações com Visibilidade de Conexões e Contenção da Rede					
22.	Solução de microssegmentação, visibilidade e proteção de Rede, baseada em Software, para controle de movimentação lateral em ambiente corporativo de servidores, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	1.500		
23.	Solução de microssegmentação, visibilidade e proteção de Rede, baseada em Software, para controle de movimentação lateral em ambiente corporativos em Containers, incluindo garantia e atualização de versão por 24 (vinte e quatro) meses	Unidade	50		
24.	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 22	Unidade	1.500		
25.	Serviço especializado para instalação, migração e suporte preventivo/corretivo por 24 (vinte e quatro) meses para o item 23	Unidade	50		

26.	Treinamento oficial	Serviço	15		
	B = Valor Total Grupo 2				
	A + B= VALOR TOTAL (Grupo 1 e 2)				

CLÁUSULA III – CLÁUSULA TERCEIRA – DO ÓRGÃO GERENCIADOR E PARTICIPANTES

3.1. O órgão gerenciador será a Secretaria Municipal de Inovação e Tecnologia – SEMIT.

3.2. Além do órgão gerenciador, são órgãos participantes do registro de preços:

2.1.1 Secretaria do Governo – SEGOV

2.1.2 Gabinete do Vice-Prefeito – GABVP

2.1.3 Controladoria Geral do Município de Salvador – CGM

2.1.4 Procuradoria Geral do Município do Salvador – PGMS

2.1.5 Casa Civil

2.1.6 Secretaria Municipal da Comunicação – SECOM

2.1.7 Secretaria Municipal de Gestão – SEMGE

2.1.8 Secretaria Municipal de Inovação e Tecnologia – SEMIT

2.1.9 Secretaria Municipal da Fazenda – SEFAZ

2.1.10 Secretaria Municipal de Desenvolvimento Urbano – SEDUR

2.1.11 Secretaria Municipal de Sustentabilidade, Resiliência, Bem-estar e Proteção Animal– SECIS

2.1.12 Secretaria Municipal de Cultura e Turismo – SECULT

2.1.13 Secretaria Municipal de Desenvolvimento Econômico, Emprego e Renda – SEMDEC

2.1.14 Secretaria Municipal da Educação – SMED

2.1.15 Secretaria Municipal da Saúde – SMS

2.1.16 Secretaria Municipal de Promoção Social, Combate à Pobreza, Esportes e Lazer – SEMPRE

2.1.17 Secretaria Municipal de Reparação – SEMUR

2.1.18 Secretaria Municipal de Políticas para Mulheres, Infância e Juventude – SPMJ

2.1.19 Secretaria Municipal de Infraestrutura e Obras Públicas – SEINFRA

2.1.20 Secretaria Municipal de Manutenção da Cidade – SEMAN

2.1.21 Secretaria Municipal de Mobilidade – SEMOB

2.1.22 Defesa Civil de Salvador – CODESAL

2.1.23 Fundação Cidade Mãe – FCM

2.1.24 Fundação Gregório de Matos – FGM

2.1.25 Fundação Mário Leal Ferreira – FMLF

2.1.26 Guarda Civil Municipal – GCM

2.1.27 Superintendência de Trânsito de Salvador – TRANSALVADOR

2.1.28 Superintendência de Obras Públicas – SUCOP

2.1.29 Agência Reguladora e Fiscalizadora dos Serviços Públicos de Salvador – ARSAL

CLÁUSULA VI –REGISTROS FORMALIZADOS

4.1 Ao participar do procedimento licitatório, o fornecedor obriga-se ao cumprimento de todos os encargos estabelecidos na presente ARP, nos exatos termos do resultado final obtido no procedimento licitatório, quanto ao preço, a quantidade e as especificações do objeto registrado, integrando e complementado a presente ARP os seguintes documentos,

os quais devem ser totalmente observados e cumpridos:

4.2 Termo de Referência contendo as especificações técnicas completas e todas as condições gerais de execução do objeto.

4.3 Proposta(s) comercial(is) do(s) particular(es) cujo(s) preço(s) conta(m) registrado(s).

CLÁUSULA V – CADASTRO RESERVA DE FORNECEDORES.

5.1 A formação de CADASTRO RESERVA vincula o(s) licitante(s) ao(s) preço(s) da proposta do titular, obrigando-se a assumir a titularidade em caso de cancelamento do registro do titular, observada a ORDEM DE CLASSIFICAÇÃO.

5.2 A alteração da titularidade do registro dependerá da comprovação das condições de participação do particular registrado no cadastro reserva, da avaliação da qualidade do objeto indicado na sua proposta e do cumprimento das condições de habilitação, nos termos fixados no edital do certame.

5.3 Caberá ao agente de contratação responsável pelo julgamento do certame para seleção do titular da presente ARP realizar o procedimento de análise dos critérios indicados no item anterior.

5.4 Havendo alteração da titularidade do registro com base no CADASTRO RESERVA, deverá a ARP ser republicada para fins de eficácia.

CLÁUSULA VI – VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

1.1 A presente ARP tem vigência de 12 MESES, contados a partir da data da sua publicação, podendo ser prorrogado para até 24 MESES, nos termos permitidos no art. 84 da Lei 14.133/2021.

1.2 A prorrogação da vigência da ARP dependerá da concordância das partes e de comprovação da vantajosidade dos preços.

1.3 A prorrogação da vigência da ARP será registrada mediante termo de prorrogação pactuado pelas partes nos autos de gestão da ARP.

1.4 A prorrogação da vigência da ARP deverá ser publicada e divulgada nos termos previstos no item 8.1 deste documento.

CLÁUSULA VII – CONTRATAÇÕES FUTURAS

7.1 As contratações decorrentes da presente ARP poderão ser realizadas diretamente pelo órgão gerenciador, ou por cada um dos participantes (se houver), observados os quantitativos respectivamente previstos para cada procedimento de licitação, e as demais exigências e formalidades previstas na legislação e na jurisprudência do TCU.

7.2 Poderá haver, a critério do órgão gerenciador e desde que haja expressa concordância dos interessados envolvidos, REMANEJAMENTO DE QUANTITATIVOS previstos na ARP, nos termos da IN nº 06/2014 SLTI/MP, o qual será formalizado nos autos de gestão da ARP por despacho da autoridade competente e publicado no DOM.

7.3 Em caso de licitação com critério de julgamento por GRUPO DE ITENS, as contratações futuras deverão ser realizadas, em regra, de forma proporcional para todos os itens de cada grupo, salvo justificativa técnica e desde que o valor registrado seja igual

ou inferior aos preços contidos nas propostas dos demais licitantes e compatíveis com os preços de mercado, nos termos contidos no art. 82, § 2º, da Lei 14.133/2021.

CLÁUSULA VIII – VÍNCULOS DA ARP

8.1 A existência desta ARP não obriga a Administração a contratar, facultando-se a realização de licitação específica para a aquisição pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições.

8.2 O titular do registro de preços vincula-se integralmente, durante a vigência da ARP, ao cumprimento das obrigações contidas na ARP, bem como à formalização das contratações dela decorrentes, salvo cancelamento ou rescisão do registro, sob pena de sofrer as sanções administrativas previstas nesta Ata.

CLÁUSULA IX – OBRIGAÇÕES DO FORNECEDOR

9.1 O FORNECEDOR cujo preço conste registrado na presente ARP obriga-se a:

9.1.1 Assinar a ata, no prazo máximo de 05 dias úteis, contados da convocação;

9.1.2 Indicar, no prazo máximo de 05 dias corridos, a concordância ou não em relação à(s) solicitação(ões) de adesão por órgão ou entidade da Administração Pública não participante, indicando expressamente que tal contratação não prejudicaria as obrigações presentes e futuras assumidas para com o ÓRGÃO GERENCIADOR e os participantes;

9.2 Observar rigorosamente todas as especificações técnicas, marcas, modelos, condições e prazos fixados no Termo de Referência (ou Projeto Básico) integrante da presente ARP, como também na sua respectiva proposta de preços, ressalvado prova idônea da ocorrência superveniente de fato impeditivo ou dificultador do cumprimento da obrigação, devidamente aceito pelo ÓRGÃO GERENCIADOR, que justifique o fornecimento de bem de qualidade semelhante ou superior, ou a execução de forma diversa que resulte em igual ou superior resultado à contratante;

9.3 Providenciar a imediata correção de deficiências, falhas ou irregularidades constatadas pela(s) CONTRATANTE(S) referentes às condições firmadas na presente ARP;

9.4 Fornecer, sempre que solicitado, no prazo máximo de 05 dias corridos, documentação de habilitação e qualificação cujas validades encontrem-se vencidas;

9.5 Prover condições que possibilitem o atendimento das obrigações firmadas a partir da data de homologação do procedimento licitatório;

9.6 Ressarcir os eventuais prejuízos causados aos órgãos contratantes e/ou a terceiros, provocados por ineficiência ou irregularidades cometidas na execução das obrigações assumidas na ARP;

9.7 Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato;

9.8 Manter, durante a vigência da presente ata, em compatibilidade com as obrigações assumidas na proposta, todas as condições de participação e de habilitação exigidas na licitação.

CLÁUSULA X – PUBLICIDADE E DIVULGAÇÃO

10.1 A formalização da ARP, como também suas possíveis alterações, prorrogações, cancelamento e rescisões, serão publicados e divulgados no PNCP – Portal Nacional de Contratações Públicas, bem como, em Jornal de Grande Circulação e Diário Oficial do Município de Salvador.

CLÁUSULA XI – ALTERAÇÕES DOS PREÇOS REGISTRADOS

11.1 Em caso de prorrogação da ARP, os preços registrados poderão ser REAJUSTADOS, para mais ou para menos, com base na variação anual do IPCA (IBGE), ou outro índice que venha a sucedê-lo, desde que decorridos 12 MESES, contados da assinatura da ARP.

11.2 A qualquer tempo, o preço registrado poderá sofrer REVISÃO em decorrência de comprovado desequilíbrio econômico-financeiro ocorrida no mercado, cabendo ao ÓRGÃO GERENCIADOR providenciar a pactuação/negociação de novo valor compatível com o de mercado, para cada ITEM/GRUPO do objeto registrado.

11.3 Caberá a parte prejudicada a demonstração do impacto efetivo nos custos em decorrência da álea econômica extraordinária havida no mercado, não cabendo revisão de preços em casos de variação inflacionária ordinária, observando-se as regras previstas no art. 124 da Lei 14.133/2021.

11.4 Não havendo acordo em relação a pactuação/negociação do preço registrado, será o respectivo registro CANCELADO/REVOGADO, por cada ITEM/GRUPO do objeto registrado, sem aplicação de qualquer sanção ao particular, mantendo-se hígidas e vigentes as contratações já formalizadas ou solicitadas, bem como os demais itens/grupos não afetados pelo desequilíbrio de preços de mercado.

11.5 Em caso do CANCELAMENTO, e havendo CADASTRO RESERVA para o respectivo ITEM/GRUPO, deverão ser realizados os procedimentos previstos no item 4 desta ARP.

11.6 Toda alteração da presente ARP será publicada e divulgada, nos termos fixados no item 8.2 desta ARP.

CLÁUSULA XII – SANÇÕES ADMINISTRATIVAS POR DESCUMPRIMENTO DE OBRIGAÇÕES CONTIDAS NA ARP

12.1 As empresas com preços registrados nesta ARP e signatárias dos respectivos contratos estarão sujeitas às sanções administrativas previstas no Edital, além das penalidades previstas entre o artigo 155 a 163 da Lei 14.133/2023, sem prejuízo de outras previstas em legislação pertinente e da responsabilidade civil e criminal que seus atos ensejarem.

12.2 As sanções do artigo 156 da Lei 14.133/2021 serão aplicadas, observadas os seguintes parâmetros:

MULTA

12.1.1 por atraso na entrega do objeto fica o fornecedor sujeito a multa de 0,5% (meio por cento) por dia de atraso, incidente sobre o valor total da nota de empenho até o efetivo cumprimento da obrigação, limitado a trinta dias;

12.1.2 em caso de inexecução parcial ou de qualquer outra irregularidade do objeto poderá ser aplicada multa de 10% (dez por cento) calculada sobre o valor total da nota de empenho;

12.1.3 transcorridos 30 (trinta) dias do prazo de entrega estabelecido na nota de empenho, será considerado rescindido o contrato, cancelado o registro de preços e aplicada multa de 10% (dez por cento) por inexecução total, calculada sobre o valor total da contratação;

12.1.4 A penalidade pecuniária aplicada será descontada dos pagamentos eventualmente devidos pela administração pública ou, caso inexista saldo, cobrada através de ação judicial;

12.1.5 Não será aplicada multa se, comprovadamente, o atraso do atendimento, advir de caso fortuito ou motivo de força maior.

12.1.6 Advertência e anotação restritiva no Cadastro de Fornecedores;

12.1.7 Impedimento temporária do direito de licitar ou de contratar com a Administração Pública.

12.1.8 Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

12.1.9 A aplicação das penalidades ocorrerá depois de garantida a ampla defesa aos interessados, no prazo estabelecido na Lei de Licitações, a contar da intimação do ato.

12.1.10 Ao órgão gerenciador caberá a aplicação de sanções administrativas em relação ao descumprimento direto de obrigação contida nesta ARP, como também aos contratos por ele firmados em decorrência do presente registro de preços.

12.1.11 Cabe a cada órgão ou entidade participante a realização de procedimento para fins de apuração de responsabilidade e aplicação de sanções administrativas nos casos de inadimplemento em suas próprias contratações, comunicando ao gerenciador para fins de registro quaisquer sanções aplicadas.

CLÁUSULA XIII – CANCELAMENTO/REVOGAÇÃO E RESCISÃO DA ARP

13.1 registro de preços poderá ser CANCELADO/REVOGADO, por ITEM/GRUPO, por iniciativa do ÓRGÃO GERENCIADOR, quando:

13.1.1 Não houve acordo entre as partes para pactuação/negociação de novo preço nos casos de comprovado desequilíbrio econômico-financeiro em relação ao mercado, conforme regras previstas no item 22 desta ARP, Lei 14.133/2021 e no Decreto nº 7.892/2013, e alterações posteriores.

13.1.2 Por iniciativa do próprio titular do registro, desde que apresente solicitação formal, bem como haja comprovação de situação que impossibilite o cumprimento das exigências insertas nesta ARP, tendo em vista fato superveniente, decorrente de caso fortuito ou força maior, aceito pelo ÓRGÃO GERENCIADOR.

13.1.3 Presentes razões de conveniência e oportunidade ao interesse público, devidamente justificadas.

13.1.4 O registro de preços poderá ser RESCINDIDO, por iniciativa do ÓRGÃO GERENCIADOR, observada a gravidade da conduta e os reflexos em relação ao interesse público, quando o titular do registro:

13.1.5 Não executar de forma total ou parcial qualificada as obrigações presentes nesta ARP;

13.1.6 Recusar-se a assinar o instrumento contratual no prazo estabelecido, salvo por motivo devidamente justificado e aceito pelo órgão ou entidade Contratante;

13.1.7 Der causa à rescisão administrativa de dois ou mais contratos firmados com base nesta ARP;

13.1.8 Não mantiver as condições de participação e de habilitação exigidas na licitação, salvo irregularidade temporária e sanável em até 30 DIAS;

13.1.9 Sofrer sanção prevista nos incisos III ou IV do artigo 156 da Lei nº 14.133/2021, ou no art. 7º da Lei nº 10.520/2002;

13.1.10 O cancelamento/revogação do registro, assegurados o contraditório e a ampla defesa, deverá ser formalizado mediante competente processo administrativo.

13.1.11 Havendo cancelamento/revogação do registro, não caberá a aplicação de qualquer espécie de sanção administrativa ao titular do registro.

13.1.12 O cancelamento/revogação do registro na hipótese prevista no item 11.3 desta ARP não poderá ser aceita em prejuízo ao interesse público.

13.1.13 A rescisão do registro de preços será determinada em decisão unilateral e fundamentada do ÓRGÃO GERENCIADOR, garantido o contraditório e a ampla defesa em processo administrativo.

13.1.14 A rescisão do registro de preços poderá ensejar a abertura de procedimento de apuração da responsabilidade e aplicação de sanções administrativas em face do titular do registro.

CLAÚSULA XIV – DO PAGAMENTO

14.1 O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Edital.

14.2 Do Recurso Financeiro.

14.2.1 As despesas decorrentes da execução da presente licitação correrão à conta dos recursos consignados ao orçamento dos órgãos indicados no subitem 2.1 do Edital, do presente exercício, devidamente ajustadas nas dotações do exercício subsequente.

14.3 Somente serão pagos os valores correspondentes aos bens/serviços efetivamente entregues/realizados e atestados na forma deste instrumento convocatório.

14.4 As notas fiscais serão liberadas para pagamento somente quando acompanhadas do relatório de recebimento, devidamente assinado e carimbado pelo funcionário responsável. Deverão constar também na nota fiscal os dados bancários e número do empenho.

CLÁUSULA XV – DAS DISPOSIÇÕES FINAIS

15.1 Integra esta Ata, o Edital de registro de preço para suprir a demanda da PMS, e as propostas das empresas classificadas no certame supranumerado.

15.2 Fica eleito o foro de Salvador (BA), para dirimir quaisquer questões decorrentes da utilização da presente ATA.

15.3 Os casos omissos serão resolvidos de acordo com a Lei nº. Lei 14.133/2021, Lei Municipal nº 4.484/92, no que couber, Decretos Municipais n.º 15.984/05 e 24.900/2014

(alterado pelo Decreto nº 25.696/2014), além do que mais for exigido no Edital e em seus Anexos, e demais normas aplicáveis.

Salvador, _ de _____de 2026

_____

SECRETARIA MUNICIPAL DE INOVAÇÃO E TECNOLOGIA

_____

FORNECEDOR/PROMITENTE

SECRETARIA MUNICIPAL DE INOVAÇÃO E TECNOLOGIA – SEMIT PREGÃO ELETRÔNICO Nº 007/ 2026

ANEXO X - MINUTA DE CONTRATO

O **MUNICÍPIO DO SALVADOR**, através da **_____,** inscrita no CNPJ sob o Nº

_____, com sede na _____, neste ato representada pelo Sr. Secretário,

_____, nomeado pelo Decreto _____, doravante denominada CONTRATANTE, do outro lado, a empresa _____, com sede _____, inscrita no CNPJ. sob n.º

_____, neste ato representada pelo seu representante legal, doravante denominada simplesmente CONTRATADA, tem entre si acordados os termos deste contrato, cuja celebração foi autorizada mediante ato homologatório às fls. _____ do processo administrativo nº_____/____, sujeitando-se as partes às Leis nº 14.133/21, Lei Municipal nº 4.484/92, está no que couber, e demais normas aplicáveis, mediante as cláusulas e condições que anunciam a seguir:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1 Contratação através de sistema de registro de preços objetivando a formalização de ATA com o vencedor do certame, visando a contratação de Solução de Cybersegurança para servidores, estações de trabalho e demais sensores de rede com gerenciamento da superfície de risco e microsegmentação de aplicações com visibilidade de conexões e contenção da rede, para a infraestrutura da SEMIT, na modalidade de subscrição de licença, incluindo suporte técnico no regime 24x7 (vinte e quatro horas por dia, sete dias por semana) e garantia de atualização das versões pelo período de 24 meses, contemplando também, instalação, configuração e treinamento de acordo com as especificações técnicas mínimas e detalhamentos consignados neste Termo de Referência (TR) e seus anexos, com a conveniência e necessidade da Prefeitura Municipal de Salvador – PMS, conforme as especificações, quantitativas e qualitativas e todas as demais condições gerais discorridas neste Termo de Referência (TR).

2. CLÁUSULA SEGUNDA – DA VIGÊNCIA DO CONTRATO

2.1 O prazo de vigência do contrato será de 12 (doze) meses, contando da data de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos, até o limite previsto, conforme arts. 106 e 107 na Lei nº 14.133/21.

3. CLÁUSULA TERCEIRA – DAS CONDIÇÕES DE PAGAMENTO

3.1 O valor global do presente Contrato é de R$ _____ inclusas todas as despesas como tributos, emolumentos, contribuições sociais, fiscais, parafiscais e quaisquer outras que forem devidas.

3.2 O pagamento será realizado pela contratante, através de crédito em conta corrente, obrigatoriamente mantida junto ao Banco Bradesco, consoante determinação do Decreto Municipal n.º 23.856/2013 (arts. 1º a 4º), com observância das exceções ali

previstas (art. 5º, parágrafo único), a qual deverá ser indicada na declaração fornecida pelo estabelecimento bancário, na forma do disposto no art. 4º, § 2º do Decreto Municipal 13.991/2002, no prazo de até 20 (vinte) dias úteis, contados da apresentação da Nota Fiscal/Fatura, em conformidade com a legislação vigente, mediante a apresentação dos documentos fiscais exigíveis e declaração de não existência de débitos registrados no CADIN Municipal, conforme Decreto Municipal nº 24.419/2013.

3.3 Nenhum pagamento será efetuado à contratada enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito a reajustamento de preço ou correção monetária.

3.4 A CONTRATANTE reserva-se o direito de não efetivar o pagamento se, no ato do "atesto", o serviço não estiver condizente com especificação requerida, até que seja promovida sua regularização;

3.5 Deverão constar, obrigatoriamente no corpo da Nota Fiscal, as seguintes informações:

3.5.1 Descrição dos serviços/produtos, preço total e data de emissão;

3.5.2 Valor total, com as deduções de impostos devidos;

3.5.3 Número do contrato;

3.5.4 Período dos serviços prestados;

3.6 Os pagamentos ficam condicionados à apresentação da Nota Fiscal ou Fatura emitida, acompanhada das Certidões que comprovem sua regularidade fiscal perante a Fazenda Federal, Estadual, Municipal, Certificado de Regularidade do FGTS – CRF, bem como certidão trabalhista;

3.7 Os pagamentos serão mensais incluídas todas as despesas com tributos, emolumentos, contribuições sociais, fiscais, parafiscais e quaisquer outras que forem devidas.

3.8 No valor da contratação deverá estar incluso todos os encargos sociais, fiscais, trabalhistas, tributários, estipulados na legislação fiscal e trabalhista, materiais de consumo, equipamentos necessários, despesas com passagens e diárias e outras que se façam necessárias para a realização do objeto contratado.

4. CLÁUSULA QUARTA – DA FONTE DE RECURSOS

4.1 As despesas decorrentes da presente licitação correrão à conta dos recursos previstos no orçamento para o exercício de 2026, na seguinte dotação orçamentária:

4.1.1 Unidade Gestora:

4.1.2 Projeto/Atividade:

4.1.3 Elemento de Despesa:

4.1.4 Fonte de Recurso:

5. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

5.1 Não será admitida a subcontratação do objeto contratual.

6. CLÁUSULA QUINTA – DO SIGILO DAS INFORMAÇÕES

6.1 Todas as informações relativas à CONTRATANTE e constantes do cadastro da CONTRATADA deverão ser tratadas como confidenciais e somente poderão ser fornecidas quando solicitadas:

6.1.1 Pela CONTRATANTE;

6.1.2 Em decorrência de determinação judicial.

6.2 Os conhecimentos, dados e informações de propriedade do Município, relativos a aspectos econômico- financeiros, tecnológicos e administrativos, tais como produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do presente Edital, constituem informação privilegiada e como tal, tem caráter de confidencialidade, só podendo ser utilizados, exclusivamente, no cumprimento e execução das condições estabelecidas neste Contrato, sendo expressamente vedado à CONTRATADA:

6.2.1 Utilizá-los para fins outros, não previstos neste Instrumento;

6.2.2 Repassá-los a terceiros e empregados não vinculados diretamente ao objeto proposto.

7. CLÁUSULA SEXTA – DA DESCRIÇÃO DOS PRODUTOS E SERVIÇOS

7.1 LOTE ÚNICO

7.1.1 Grupo 01 – Solução de Cybersegurança para Servidores, estações de trabalho com gerenciamento da superfície de risco:

7.1.1.1 A aquisição de soluções de Cybersegurança objetos desta licitação possui, como intuito, prevenir a contaminação por códigos maliciosos, suas variantes e demais ameaças cibernéticas, nos computadores dos Órgãos da Prefeitura Municipal do Salvador, mitigando o risco e preservando o sigilo, a integridade e a disponibilidade das informações.

7.1.1.2 O dinamismo no surgimento de novas tecnologias e a crescente demanda surgem as necessidades permanentes em manter-se alta disponibilidade, alto desempenho, segurança e controle para que todos os usuários, das redes dependentes direta ou indiretamente da Secretaria Municipal de Inovação e Tecnologia – SEMIT, possam exercer suas atividades de rotina, proporcionando melhor qualidade nas ações corporativas da PMS.

7.1.1.3 A expansão das ferramentas do fabricante TREND MICRO atualmente em uso na SEMIT com novas tecnologias do fabricante, visam a continuidade das adoções de providências necessárias para agilizar a tomada de decisões que exigem celeridade, otimizando as ações da máquina administrativa, reduzindo os riscos de indisponibilidade dos sistemas, reduzindo a probabilidade de êxito em ataques cibernéticos, proporcionando monitoração contínua e efetiva da

infraestrutura e dos serviços de TIC, além de ampliar a proteção dos dados prevista no Marco Civil da Internet e na Lei Geral de Proteção de dados, LGPD.

7.1.1.4 A importância da integração entre essas ferramentas existentes e novas tecnologias a serem adquiridas deve ser garantida para preservar uma gerência global sobre as mesmas e a capacidade de correlacionar eventos detectados nos diversos sensores da solução. A contratação destas ferramentas justifica-se para garantir a segurança do ambiente de TIC da SEMIT e das Unidades da Prefeitura Municipal do Salvador.

7.1.2 Grupo 2 – Solução de Cybersegurança para Microsegmentação de aplicações com visibilidade de conexões e contenção da rede

7.1.2.1 Implementação de mecanismos de isolamento granular de cargas de trabalho e seus fluxos de rede em função da obrigatoriedade dos processos individuais utilizados nos servidores e containers, com o objetivo de reduzir a superfície de ataque, garantir maior visibilidade e divisão da rede em segmentos menores, restringindo tráfego Leste-Oeste, fortalecer a contenção de ameaças por meio das políticas de segurança dinâmicas.

7.1.2.2 A utilização de solução de microsegmentação aumenta a proteção de rede e torna-se fundamental para garantir proteção de ambientes complexos e altamente distribuídos, como os encontrados nos sistemas governamentais, que venha garantir eficiência na detecção de ameaças e violações, reduzindo o tempo de resposta a incidentes.

7.1.2.3 Insights com busca capaz detectar plataformas e dispositivos de alto risco no ambiente.

7.1.2.4 Orquestração de políticas de segurança detalhadas para cada segmento da rede, baseado na visibilidade histórica dos fluxos de rede e da comunicação com processos existentes em função da ampla e granular proteção dos segmentos de rede que atuam de forma independente para garantia de segurança dos ambientes. As aplicações destas políticas garantem maior agilidade e flexibilidade na resposta de incidentes, permitindo de forma granular isolar rapidamente um segmento de rede inteiro, bem como isolar apenas o processo de comunicação, permitindo assim a continuidade de serviços ativos dentro do mesmo servidor infectado.

7.1.2.5 Prevenção de movimentação lateral com detecção de brechas através da microsegmentação, com visibilidade efetiva e monitoramento de comunicação para todas as cargas de trabalho.

7.1.2.6 Ampla cobertura de plataformas para tecnologias legadas e sistemas mais recentes.

7.1.2.7 A adoção de uma solução de Microsegmentação, Visibilidade e Contenção do Tráfego de Rede é particularmente relevante no contexto da SEMIT, para garantia da integridade dos dados sensíveis e continuidade dos serviços essenciais, com controle, proteção, e visibilidade das interações entre os sistemas do ambiente e para com o ambiente controlado pela aplicação, o que

aprimora e otimiza a segurança em geral através do gerenciamento granular de redes distribuídas e complexas. Essa abordagem moderna de segurança fortalece o ecossistema digital, alinhando-se às demandas estratégicas de proteção de dados e garantindo uma infraestrutura mais resiliente, menos vulnerável a falhas, ataques internos e externos.

7.1.2.8 Pode-se elencar abaixo os pontos de destaque aos benefícios projetados:

7.1.2.9 Convergência tecnológica desejada e necessária à implementação de todos os eixos e estratégias da Administração Municipal.

7.1.2.10 Alinhamento estratégico de planejamento, orientados pela Secretaria Municipal de Inovação e Tecnologia – SEMIT;

7.1.2.11 Maior qualidade da dos serviços de TIC da PMS e da Secretaria Municipal de Inovação e Tecnologia – SEMIT;

7.1.2.12 Gerenciamento e segurança eficiente e proativo da rede e serviços de TIC da PMS e da Secretaria Municipal de Inovação e Tecnologia – SEMIT;

7.1.2.13 Monitoração contínua e efetiva da infraestrutura e dos serviços de TIC da PMS e da Secretaria Municipal de Inovação e Tecnologia – SEMIT;

7.1.2.14 Aumento do grau de satisfação dos usuários com os serviços de TIC da PMS;

7.1.2.15 Ampliar a visibilidade e o controle do uso da Infraestrutura e dispositivos aderente ao Plano Estratégico orientada à Governa e Políticas de Acesso;

7.1.2.16 Ampliar proteção contra riscos iminentes de ciberataques associados às ameaças de Ransomware, tais como WannaCry e Petya;

7.1.2.17 Ampliar proteção contra risco potencial associado a conexões indevidas e maliciosas às aplicações;

7.1.2.18 Ampliar proteção contra risco potencial associado a Movimentação Lateral e conexões de rede;

7.1.2.19 Ampliar proteção contra risco latente nos sistemas operacionais legados;

7.1.2.20 A utilização do sistema de registro de preços justifica-se por tratar-se de objeto cuja contratação será de forma parcelada e sem garantia de saque total, em função das incertezas acerca do tempo e da efetivação da implantação devido à complexidade do ambiente operacional refletida na diversidade de versões dos sistemas existentes no parque tecnológico.

8. CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

8.1 Assegurar a correta integração e funcionalidade dos serviços, em função do projeto e das especificações técnicas constantes neste Termo de Referência.

8.2 Efetuar inspeção/vistoria do local onde ocorrerá a instalação dos equipamentos, conforme indicação da SEMIT, para verificar os detalhes técnicos de execução.

8.3 Apresentar, ao final do serviço de instalação, o relatório de conclusão do projeto, contendo os seguintes documentos:

8.4 Memorial descritivo de todo o serviço e produtos utilizados;

8.5 Relação de licenças das soluções e serviços.

8.6 Não transferir a outrem, no todo ou em parte, o objeto do presente Termo de Referência, sem prévia e expressa anuência da SEMIT.

8.7 Manter toda estrutura de pessoal e ferramental necessários para execução do contrato, incluindo, fornecimento e serviços, independentemente da demanda definida pela CONTRATANTE.

8.8 Responsabilizar-se por toda a logística (transporte e comunicação) necessária à execução do fornecimento e dos serviços propostos, em todo o Município do Salvador, para atendimento imediato às solicitações da SEMIT, conforme a demanda.

8.9 Arcar com todas as despesas provenientes da limpeza dos locais de instalações e adequações necessárias.

8.10 Manter preposto para representá-la durante a execução dos serviços ora tratados, desde que aceito pela SEMIT.

8.11 Empregar, na execução dos serviços, a equipe técnica indicada na proposta, que poderá ser alterada mediante solicitação de autorização à CONTRATANTE.

8.12 Responder por quaisquer danos que venha a causar à União, Estado, Município ou a terceiros, em função do objeto do contrato firmado, bem como por todos os danos e prejuízos decorrentes de paralisações na execução dos serviços, salvo na ocorrência de motivo de força maior, apurados na forma da legislação vigente, e desde que comunicados à CONTRATANTE no prazo de 48 (quarenta e oito) horas do fato, ou da ordem expressa e escrita da CONTRATANTE.

8.13 Arcar com todas as despesas, diretas ou indiretas, decorrente do cumprimento das obrigações assumidas sem qualquer ônus à CONTRATANTE.

8.14 Arcar integralmente com todas as despesas inerentes à execução dos serviços, tais como, combustíveis, manutenção, seguros, taxas, impostos, tributos e salários.

8.15 Manter, durante toda a execução do Contrato, as mesmas condições da habilitação e qualificação exigidas nesta Licitação.

8.16 Efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente Contrato, bem como observar e respeitar as legislações Federal, Estadual e Municipal relativas ao objeto do Contrato.

8.17 Manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e mão de obra para execução dos serviços.

8.18 Reparar, corrigir, remover, reconstruir ou substituir, total ou parcialmente, às suas expensas, os equipamentos e serviços objeto do fornecimento em que se verifiquem vícios, defeitos ou incorreções, resultantes de execução irregular, do emprego de materiais ou equipamentos inadequados, se for o caso, ou não correspondentes ao serviço.

8.19 Apresentar composição de preços detalhada para aprovação da CONTRATANTE.

8.20 Acatar as normas e condições deste Termo de Referência e seus anexos, independente de transcrição.

8.21 Disponibilizar um profissional que acompanhará as ações junto à SEMIT para recebimento de Ordens de Serviço, informações, contato com os técnicos responsáveis pelos serviços, coordenação, administração e supervisão do seu pessoal, bem como de qualquer comunicação junto à CONTRATANTE.

8.22 Permitir e facilitar a atuação de auditores e inspetores de qualquer natureza, sempre que necessário.

8.23 Arcar com indenização pecuniária decorrente dos danos morais ou materiais causados por seus empregados em bens patrimoniais da CONTRATANTE, bem como por desaparecimento de quaisquer objetos e valores encontrados em suas dependências, de quem quer que seja, desde que comprovado dolo ou culpa, do empregado da CONTRATADA.

8.24 Afastar ou substituir dentro de 24 (vinte e quatro) horas, sem ônus para a CONTRATANTE, qualquer funcionário que, por solicitação justificada da Fiscalização, não tenha condição de continuar a participar da execução dos serviços.

8.25 Realizar regularmente os exames de saúde dos seus empregados, na forma da lei, assim como arcar com todas as despesas decorrentes de transporte, alimentação, inclusive seguro de vida contra os riscos de acidentes de trabalho e outras especificadas nos dissídios ou convenções coletivas.

8.26 Cada prestador de serviço da contratada deverá apresentar-se uniformizado, com fardamento padrão fornecido pela CONTRATADA, e portando crachá de identificação.

8.27 Manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente do fornecimento e dos serviços objeto deste Contrato.

8.28 Responder perante à CONTRATANTE pela conduta, frequência, pontualidade e assiduidade de seus empregados e efetuar as substituições daqueles que venham a se ausentar do serviço, por motivo justificado ou não, sem nenhum ônus para a CONTRATANTE, bem como comunicar à SEMIT, antecipadamente, todo e qualquer afastamento, substituição ou inclusão de qualquer um dos seus empregados vinculados à execução do presente Contrato.

8.29 Zelar pela boa e completa execução dos serviços e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pela SEMIT, atendendo prontamente às observações e exigências que lhe forem solicitadas.

8.30 Não efetuar despesa, celebrar acordos, fazer declarações ou prestar informações em nome da SEMIT.

8.31 Comunicar imediatamente ocorrências de qualquer natureza que impeçam o bom andamento do serviço.

9. CLÁUSULA OITAVA – DAS OBRIGAÇÕES DA CONTRATANTE

9.1 Efetuar o empenho da despesa, garantindo o pagamento das obrigações assumidas.

9.2 Acompanhar e fiscalizar a entrega dos produtos contratados, bem como atestar na nota fiscal/fatura a efetiva entrega dos itens contratados e o seu aceite.

9.3 Aplicar à CONTRATADA as sanções regulamentares e contratuais, garantindo o contraditório e a ampla defesa.

9.4 Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

9.5 Verificar minuciosamente, no prazo fixado, a conformidade dos produtos recebidos provisoriamente com as especificações constantes deste Termo de Referência e da proposta, para fins de aceitação e recebimento definitivos.

9.6 Notificar o fornecedor, por escrito, sobre imperfeições, falhas ou irregularidades constantes nos objetos fornecidos, para que sejam corrigidos.

9.7 Verificar se os softwares entregues pela CONTRATADA estão em conformidade com as especificações técnicas e funcionalidades constantes deste Termo de Referência, podendo sustar, recusar, mandar fazer ou desfazer qualquer fornecimento de software que esteja em desacordo com as especificações técnicas descritas neste Termo de Referência.

10. CLÁUSULA NONA - DAS RESPONSABILIDADES

10.1 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resulte de imperfeições ou vícios, e, na ocorrência desta, não implica em corresponsabilidade da Contratante ou de seus agentes e prepostos.

10.2 A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda vinculados a execução do presente contrato, bem como por qualquer dano causado a terceiros, em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

10.3 A CONTRATADA declara haver levado em conta, na apresentação de sua proposta, os tributos, contribuições fiscais, parafiscais, emolumentos, encargos sociais e todas as despesas incidentes sobre os serviços, não cabendo quaisquer reivindicações devidas a erros nessa avaliação, para efeito de solicitar revisão de preços por recolhimentos determinados pela autoridade competente.

10.4 Para todos os fins de direito, não existirá entre a PREFEITURA MUNICIPAL DE SALVADOR e os empregados da prestadora de serviços da CONTRATADA, vínculos de qualquer natureza, correndo por conta e responsabilidade única e exclusiva da CONTRATADA todas as obrigações trabalhistas, previdenciárias, FGTS, seguros e quaisquer outros encargos decorrentes das relações empregatícias existentes.

10.5 Todas as comunicações relativas ao presente Contrato serão consideradas como regularmente feitas desde que entregues ou enviadas por carta protocolada ou e-mail, devidamente confirmados.

10.6 As reuniões realizadas entre representantes credenciados das partes, bem como as ocorrências que possam ter implicações no Contrato serão registradas por escrito em forma de ata, assinada pelos presentes.

11. CLÁUSULA DÉCIMA – DA RESCISÃO

11.1 A CONTRATANTE poderá rescindir administrativamente o presente contrato nas

hipóteses previstas no art. 137º e 138º da Lei nº 14.133/2021, sem que caiba à CONTRATADA o direito a qualquer indenização, e sem prejuízo das penalidades pertinentes.

11.2 Poderá, ainda, ser rescindido pela CONTRATANTE, a qualquer tempo, mediante simples aviso à outra parte, com antecedência mínima de 30 (trinta) dias.

12. CLÁUSULA DÉCIMA PRIMEIRA - DAS SANÇÕES ADMINISTRATIVAS

12.1 A EMPRESA sujeitar-se-á, no caso de cometimento de infrações ou inadimplemento de suas obrigações, às penalidades previstas na Lei Federal n° 14.133/21, sem prejuízo das demais dominações legais, em especial as Infrações administrativas previstas no art. 155º da Lei 14.133/21, as quais serão devidamente descritas no instrumento contratual.

13. CLÁUSULA DÉCIMA SEGUNDA – DA ALTERAÇÃO CONTRATUAL E REAJUSTE

13.1 O valor do contrato poderá ser reajustado a cada 12 (doze) meses, tomando-se por base a variação do Índice de Preços ao Consumidor – IPCA-E do IBGE, ou, na sua falta, índice legalmente previsto à época.

13.2 A alteração de quaisquer das cláusulas ou condições contidas neste contrato, só poderá ser procedida através de aditivo assinado pelas partes, resguardado o disposto no art. 124º, inciso I, alíneas "a" e "b" da Lei nº14.133/21.

13.3 A CONTRATADA obriga-se a aceitar, quando solicitado pela CONTRATANTE, nas mesmas condições e dentro do prazo contratual estabelecido, os acréscimos e supressões que se fizerem necessários nos serviços, até 25% (vinte e cinco por cento) do valor inicial deste contrato, salvo as supressões resultantes de acordo celebrado entre os contratantes, previsto no artigo 125º da Lei nº14.133/21.

13.4 As alterações deverão ser devidamente justificadas e, quando se tratar de modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa do objeto, além de outros requisitos legais, deverá haver a solicitação formal do dirigente máximo da unidade municipal interessada, a comprovação de que houve aumento ou diminuição da demanda inicialmente prevista e a indicação dos recursos suficientes para fazer face ao aumento da despesa, passando a ser alterado e consolidado o quadro de equipamentos e sua alocação na respectiva unidade municipal.

14. CLÁUSULA DÉCIMA TERCEIRA - ACOMPANHAMENTO E FISCALIZAÇÃO

14.1 O responsável pela fiscalização e acompanhamento da execução dos serviços, deverá avaliar a sua qualidade, sem prejuízo das responsabilidades da CONTRATADA, podendo rejeitá-los, mediante justificativa.

14.2 A presença da fiscalização no local dos serviços não atenua nem diminui a responsabilidade do preposto da CONTRATADA no que diz respeito a qualquer ocorrência, atos irregulares ou omissões verificadas no desenvolvimento dos trabalhos a ele relacionados.

14.3 A SEMIT poderá recusar quaisquer serviços, quando entender que os mesmos estejam em desacordo com a legislação aplicável e/ou contrário aos termos do contrato

celebrado.

14.4 Ao servidor designado pela Administração para Fiscal do Contrato, caberá no acompanhamento e na fiscalização do termo de Contrato, registrar as ocorrências relacionadas com sua execução, comunicando à CONTRATADA as providências necessárias à sua regularização, as quais deverão ser atendidas de imediato, salvo motivo de força maior.

15. CLÁUSULA DÉCIMA QUARTA - DISPOSIÇÕES ANTICORRUPÇÃO

15.1 As Partes declaram ter conhecimento que estão subordinadas à lei brasileira n° 12.846, de 01 de agosto de 2013 ("Lei Anticorrupção"), tendo a legislação previsão de vedação para efetuar qualquer pagamento ou doação de qualquer coisa de valor, seja direta ou indiretamente, a uma autoridade governamental, partido político ou candidato a cargo público, com o propósito de influenciar determinado ato ou decisão no âmbito de sua capacidade oficial, ou induzi-lo a usar sua influência no sentido de obter vantagens de quaisquer natureza.

15.2 A CONTRATADA declara, ainda, que nem ela, nem qualquer outro diretor, de sua empresa é empregado, funcionário ou representante do governo nacional ou estrangeiro, partido político nacional ou estrangeiro ou candidato para algum cargo político nacional ou estrangeiro.

15.3 A CONTRATADA se compromete a zelar para que seus atos e de seus diretores, colaboradores e representantes também não violem tais normas da Lei Anticorrupção brasileira, devendo, além disso, cooperar com o MUNICÍPIO quanto a eventuais questionários de auditoria ou investigações e quanto as possíveis suspeitas de violação da lei brasileira de Anticorrupção por qualquer diretor, colaborador ou representante.

16. CLÁUSULA DÉCIMA QUINTA– DA GARANTIA CONTRATUAL

16.1 Em garantia de plena, fiel e segura execução de tudo o que se há obrigado, a CONTRATADA prestará caução correspondente a 5% (cinco por cento) sobre o valor global do objeto contratado, em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, cuja liberação ou restituição dar-se-á após a expiração deste instrumento contratual.

16.2 A garantia será obrigatoriamente revista e complementada quando houver redução da sua representatividade percentual por variação econômica do contrato ou descontos de valores devidos ao CONTRATANTE, a exemplo de multas, quando for o caso.

16.3 A garantia responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais.

16.4 O cálculo da atualização monetária do valor caucionado em dinheiro será feito aplicando-se o índice mais vantajoso para a Administração entre a data de retenção da caução e da devolução do seu valor.

16.5 A garantia deverá ser apresentada no prazo máximo de 10 (dez) dias corridos, contados da assinatura do Contrato.

17. CLÁUSULA DÉCIMA SEXTA– DAS DISPOSIÇÕES FINAIS

17.1 A CONTRATADA deverá apresentar, na data da assinatura do Contrato, nome e telefone de um profissional da empresa, o qual atuará como preposto junto à CONTRATANTE.

17.2 Em caso de cisão, fusão ou incorporação da CONTRATADA, deverá ser assegurada a continuidade do objeto.

17.3 Obriga-se a CONTRATADA ao perfeito e integral atendimento dos termos do presente Contrato, respondendo pelos danos e prejuízos que venha a causar à CONTRATANTE, por inadimplemento.

17.4 É expressamente vedada a transferência das obrigações assumidas pela CONTRATADA a terceiros.

17.5 O não exercício pelas partes, de qualquer faculdade ou garantia assegurada no contrato ou em qualquer dos documentos que o integre, não será considerado como renúncia ao direito em si ou novação, relativamente às informações subsequentes que justifiquem a sua invocação ou aplicação.

17.6 Fazem parte integrante deste Contrato independentemente de transcrição, a proposta apresentada pela CONTRATADA e a respectiva solicitação do CONTRATANTE.

17.7 Todos os serviços poderão ser executados em qualquer unidade da PMS ou em vias e espaços públicos de Salvador.

18. CLÁUSULA DÉCIMA SEXTA – DA LEGISLAÇÃO

18.1A legislação que regula a presente contratação é: Lei 8.078 de 11/09/1990 - Código de Defesa do Consumidor; Lei 10.406 de 10/01/2002 – Código Civil; Lei 8.137 de 27/12/1990 - Crime Contraordem Econômica e Relações de Consumo; Lei Federal 8429 de 02/06/1992; Lei Complementar 123 de 14/12/2006; Decreto Municipal n.º 13.991/2002, Lei 14.333/21, outras legislações quando couber.

19. CLÁUSULA DÉCIMA SÉTIMA – DO FORO

19.1As partes contratantes elegem o foro de Salvador, Estado da Bahia, como único competente para dirimir as questões que porventura surgirem na execução do presente Contrato, com renúncia a qualquer outro, por mais privilegiado que seja.

19.2E, por estarem justas e contratadas, assinam as partes, depois de lido e achado conforme, o presente contrato em duas vias de igual teor, para a sua validade e eficácia jurídicas.

Salvador, _____de _____de 2026

CONTRATANTE:

_____

Secretário CONTRATADA:

Representante Legal Testemunhas

SECRETARIA MUNICIPAL DE INOVAÇÃO E TECNOLOGIA – SEMIT PREGÃO ELETRÔNICO Nº...../ 2026

ANEXO XI - MODELOS DE DECLARAÇÕES A SEREM APRESENTADAS JUNTAMENTE COM A PROPOSTA.

A - DECLARAÇÃO NEGATIVA DE RELAÇÃO FAMILIAR OU PARENTESCO

(Nome da pessoa física/jurídica) _____, inscrita no CNPJ/CPF sob o nº _____, por intermédio de seu representante legal o(a) Sr. (a). _____, portador (a) do CPF nº _____, DECLARA, para todos os efeitos legais que:

1. não possui sócio (s) ou, no caso de sociedade anônima, diretor(es) que seja(m):

a. cônjuge(s), companheiro(s) ou tenha(m) parentesco em linha reta, colateral ou por afinidade, até o terceiro grau, ou que tenham ocupado os mencionados cargos/funções, nos 6 (seis) meses anteriores à data de abertura da sessão pública do procedimento licitatório;

b. cônjuge(s), companheiro(s) ou tenha(m) parentesco em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, com servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação deste Poder Administrativo, ou que tenham ocupado os mencionados cargos, nos 6 (seis) meses anteriores à data de abertura da sessão pública do procedimento licitatório;

2. está ciente da vedação:

a) da subcontratação, quando autorizada pelo CONTRATANTE, de pessoa física ou jurídica se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com servidor ocupante de cargo de direção, chefia ou assessoramento vinculado direta ou indiretamente a unidade situada na linha hierárquica da área encarregada da licitação, ou se deles forem companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau inclusive; e

b) b) da manutenção, aditamento ou prorrogação de contrato de prestação de serviços, caso a CONTRATADA venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento vinculados ao CONTRATANTE.

3. são verdadeiras as informações prestadas no presente documento, sob pena de responsabilidade civil, administrativa e penal.

B - DECLARAÇÃO DE CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS LEI Nº 13.709/2018

26 É vedada 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.

27 As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassadas em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018, 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.

28 As partes responderão administrativa e judicialmente, caso causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD.

29 Em atendimento ao disposto na Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), o CONTRATANTE, para a execução do serviço objeto deste Edital, terá acesso aos dados pessoais dos representantes da LICITANTE/CONTRATADA, tais como: número do CPF e do RG, endereços eletrônico e residencial e cópia do documento de identificação.

30 A LICITANTE/CONTRATADA declara que tem ciência da existência da Lei Geral de Proteção de Dados Pessoais (LGPD) e, se compromete a adequar todos os procedimentos internos ao disposto na legislação, com intuito de proteção dos dados pessoais repassados pelo CONTRATANTE.

31 A LICITANTE/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 que possa vir causar risco ou dano relevante aos Titulares de Dados Pessoais, apresentando as informações descritas nos incisos do § 1º do art. 48 da LGPD, cabendo ao CONTRATANTE as demais obrigações de comunicação previstas no referido artigo.

32 O canal de comunicação em caso de incidentes de segurança será o Comitê Gestor de Dados Pessoais.

C- DECLARAÇÃO DE INTEGRALIDADE DOS CUSTOS

A LICITANTE/CONTRATADA declara 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.

D - DECLARAÇÃO DE RESERVA DE CARGOS

A LICITANTE/CONTRATADA declara que cumprirá, caso aplicável, as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas.

E - DECLARAÇÃO DE QUE PODE USUFRUIR DOS BENEFÍCIOS DE ME E EPP.

A LICITANTE/CONTRATADA declara, para todos os efeitos legais, que, no ano-calendário de realização da licitação, não celebrou contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, para fins de obtenção dos benefícios previstos dos artigos 42 a 49 da Lei Complementar nº 123/2006.

F - DECLARAÇÃO PARA QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

Declaramos que as demonstrações abaixo correspondem a real situação da proponente. Esses índices foram obtidos no Balanço Patrimonial do último exercício social. Declaramos, ainda, que a qualquer tempo, desde que solicitado pelo licitador, nos comprometemos a apresentar todos os documentos ou informações que comprovarão as demonstrações.

Patrimônio Líquido: R$ ..... (valor por extenso) equivale a % do valor

estimado da contratação.

G - DECLARAÇÃO DE ATENDIMENTO AO INCISO XXXIII DO ART. 7º. DA CONSTITUIÇÃO FEDERAL

Declaramos, para os fins do disposto no inciso VI do art. 68 da Lei nº14.133/2021, que não empregamos menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não empregamos menor de 16 (dezesseis) anos.

Ressalva: emprega menor, a partir de 14 (quatorze) anos, na condição de aprendiz (.).

Observação: em caso afirmativo, assinalar a ressalva acima.

H - DECLARAÇÃO DE VISTORIA

A LICITANTE/CONTRATADA declara que está ciente e tem conhecimento pleno das condições e peculiaridades para a execução do objeto deste procedimento licitatório, dispensando a realização de vistoria, nos termos do art. 63, § 3º da Lei nº 14.133/2021.

I - DECLARAÇÃO DE PLENO CONHECIMENTO DO EDITAL E ANEXOS

O LICITANTE, (razão social), inscrita sob o CNPJ nº _____ com sede na _____ (endereço completo), por meio de seu representante legal, (qualificação), em atendimento ao disposto no Edital, declara para os devidos fins, que tem pleno conhecimento do Edital nº...../..... e seus Anexos e todas as informações, das condições locais e dificuldades para o cumprimento das obrigações objeto desta licitação, e ainda, que aceita como válida a situação em que se encontra para a realização dos serviços a que se refere ..... nº...../ e por ser verdade, assina a presente declaração sob as penas da lei, nos termos do inciso VI, art. 67 da Lei nº 14.133/2021.

J - DECLARAÇÃO DE QUE NÃO ESTÁ INCURSO EM IMPEDIMENTOS

A Empresa ___, declara para os devidos fins licitatórios que não incursa nos impedimentos para disputa de licitação ou execução do contrato de que trata o Art. 14 da Lei Federal

K - DECLARAÇÃO DE CONTRATOS FIRMADOS COM A INICIATIVA PRIVADA E A ADMINISTRAÇÃO PÚBLICA.

Declaro que a empresa _____, inscrita no CNPJ nº _____, Inscrição Estadual nº _____, estabelecida em_____, possui os seguintes contratos firmados com a iniciativa privada e a administração pública: NOME DO ORGÃO / EMPRESA VIGÊNCIA DO CONTRATO VALOR TOTAL DO CONTRATO

Local e data

_____

Assinatura e carimbo do emissor

EDITAL DE PREGÃO ELETRÔNICO – SEMIT Nº 003/2026
ANEXO XII
ATA DE REGISTRO DE PREÇOS

EDITAL DE LICITAÇÃO Nº__/2026 - SEMIT
PROCESSO Nº. 13202/2026
EMPRESA (razão social):
CNPJ:
ENDEREÇO:

Item	Código	un	Especificação

Preço ofertado	Preço de mercado	% Diferença preço de mercado
Locais pesquisados:		Data da pesquisa:
1		
2		
3		

Item	Código	un	Especificação

Preço ofertado	Preço de mercado	% Diferença preço de mercado
Locais pesquisados:		Data da pesquisa:
1		
2		
3		

DATA ASSINATURA/CARIMBO