EMPRESA MARANHENSE DE ADMINISTRAÇÃO PORTUÁRIA

LICITAÇÃO POR PREGÃO ELETRÔNICO N° 021/2024 – EMAP

CONSTITUI OBJETO DO PRESENTE EDITAL A CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA O FORNECIMENTO DE EVOLUÇÃO TECNOLÓGICA DE PROTEÇÃO DE BORDA, ESTAÇÕES DE TRABALHO E SERVIDORES DA EMAP - EMPRESA MARANHENSE DE ADMINISTRAÇÃO PORTUÁRIA, BEM COMO SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO, CONFORME CONDIÇÕES, QUANTIDADES E EXIGÊNCIAS ESTABELECIDAS NESTE EDITAL.

DATA e HORA DA SESSÃO DE ABERTURA DA LICITAÇÃO: 08 de julho de 2024, às 09:30 horas, horário de Brasília - DF.

RETIRADA DO EDITAL: O Edital e seus anexos estão à disposição dos interessados, no sítio www.licitacoes-e.com.br e www.emap.ma.gov.br, podendo ainda ser adquiridos gratuitamente na CSL/EMAP, durante os dias úteis, das 08:00 às 12:00 horas e das 13:00 às 17:00 horas, por meio da apresentação de dispositivo de armazenagem eletrônica (cd, pen drive etc.).

FUNDAMENTO LEGAL: A licitação reger-se-á pelas disposições do Regulamento de Licitações e Contratos da Empresa Maranhense de Administração Portuária - EMAP, da Lei Complementar n° 123, de 14 de dezembro de 2006 e alterações e Lei Federal n° 13.303, de 30 de junho de 2016.

FORMA DE EXECUÇÃO DA LICITAÇÃO: ELETRÔNICO

MODO DE DISPUTA: ABERTO

ORÇAMENTO: SIGILOSO

CRITÉRIO DE JULGAMENTO: MENOR PREÇO

REGIME DE EXECUÇÃO: EMPREITADA POR PREÇO GLOBAL

Empresa Maranhense de Administração Portuária - EMAP
Porto do Itaqui | São Luís | Maranhão | Brasil
Av. dos Portugueses | s/nº | 65085-370 | Tel.: +55 98 3216-6000
Ouvidoria: (98) 3216-6562 / ouvidoria@emap.ma.gov.br
comunicacao@emap.ma.gov.br | www.emap.ma.gov.br

SUMÁRIO

1. DO OBJETO, DO VALOR ESTIMADO E DOS PRAZOS DE EXECUÇÃO E DE VIGÊNCIA 2

2. DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO 2

3. DAS CONDIÇÕES DE PARTICIPAÇÃO 3

4. DA REPRESENTAÇÃO E DO CREDENCIAMENTO 4

5. DO ENVIO DA PROPOSTA DE PREÇOS 5

6. DA FORMULAÇÃO DOS LANCES 6

7. DO JULGAMENTO DAS PROPOSTAS 7

8. DA HABILITAÇÃO 9

9. DO ENCAMINHAMENTO DA DOCUMENTAÇÃO E DA PROPOSTA 13

10. DOS RECURSOS 14

11. DA HOMOLOGAÇÃO E CONTRATAÇÃO 14

12. DAS SANÇÕES ADMINISTRATIVAS 15

13. DA DOTAÇÃO ORÇAMENTÁRIA 15

14. DA GARANTIA DE EXECUÇÃO DO CONTRATO 18

15. DO PROGRAMA DE INTEGRIDADE 20

14. DISPOSIÇÕES GERAIS 21

EDITAL DE LICITAÇÃO PÚBLICA

PREGÃO ELETRÔNICO N° 021/2024 – EMAP

A **EMPRESA MARANHENSE DE ADMINISTRAÇÃO PORTUÁRIA - EMAP** leva ao conhecimento dos interessados que realizará licitação, na modalidade Pregão Eletrônico, pelo critério de julgamento menor preço, no modo de disputa aberto, em vista do que consta nos autos do Processo Administrativo Eletrônico n. º 1381/2024 - EMAP, de 02/05/2024, conforme descrito neste e seus anexos.

A licitação reger-se-á pelas disposições do Regulamento de Licitações e Contratos da Empresa Maranhense de Administração Portuária - EMAP, da Lei Complementar n° 123, de 14 de dezembro de 2006 e Lei Federal n° 13.303, de 30 de junho de 2016.

A Sessão Pública do Pregão terá início na data e horários abaixo indicados, ou no primeiro dia útil subsequente, na hipótese de não haver expediente na EMAP nesta data, e será processada exclusivamente por meio eletrônico, sendo necessário que as licitantes interessadas providenciem previamente o credenciamento junto ao **Banco do Brasil**, por meio do site www.licitacoes-e.com.br, para obtenção da chave de identificação e de senha:

DATA: 08/07/2024
Às 09:30hs - Horário de Brasília–DF, ou no primeiro dia útil subsequente, na hipótese de não haver expediente nesta data.
Site: www.licitacoes-e.com.br
Fones: (98) 3216-6531 / 6532 / 6533 / 6028
e-mail: csl@emap.ma.gov.br

1. DO OBJETO, DO VALOR ESTIMADO E DOS PRAZOS DE EXECUÇÃO E DE VIGÊNCIA

1.1. O objeto da presente licitação é a contratação de empresa para o fornecimento de evolução tecnológica de proteção de borda, estações de trabalho e servidores da EMAP- Empresa Maranhense De Administração Portuária, bem como serviço de instalação e configuração, conforme quantitativos e especificações do Termo de Referência, Anexo I deste Edital.

1.2. O orçamento previamente estimado para a contratação será tornado público apenas e imediatamente após a adjudicação do objeto.

1.2.1 É facultada a abertura do sigilo do orçamento na fase de negociação de preços com o primeiro colocado, desde que em ato público e devidamente justificado, no intuito de assegurar a efetividade da negociação.

1.3. O prazo de execução será de 12 (doze) meses, a contar da data indicada na Ordem de Fornecimento (OF), limitando-se ao prazo de vigência contratual.

1.4. O prazo de vigência do contrato será de 15 (quinze) meses, contados a partir da assinatura do Contrato.

1.5. A contratada terá o prazo de até 60 (Sessenta) dias corridos, a partir da data indicada na Ordem de Fornecimento, para concluir a entrega dos equipamentos.

2. DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

2.1. Qualquer cidadão ou interessado poderá solicitar esclarecimentos ou impugnar o ato convocatório do Pregão, no prazo de até 5 (cinco) dias úteis antes da data fixada para a ocorrência do certame, devendo a impugnação ser julgada e respondida em até 3 (três) dias úteis, nos termos do art. 94 do Regulamento de Licitações e Contratos da EMAP.

2.2. O pedido de impugnação poderá ser protocolizado no Setor de Protocolo da EMAP, localizado no Prédio sede da EMAP, localizado na Avenida dos Portugueses, s/n, Itaqui, São Luís-MA, ou encaminhado para o e-mail da CSL/EMAP (csl@emap.ma.gov.br), dentro do horário de expediente da EMAP, das 08:00 às 12:00 e das 13:00 às 17:00 horas.

2.3. Se procedente e acolhida a impugnação do edital, seus vícios serão sanados e nova data será designada para a realização do certame, observado o Parágrafo Único do Art. 39 da Lei Federal 13.303/16.

2.4. A entrega da proposta, sem que tenha sido tempestivamente impugnado o presente Edital, implicará na plena aceitação, por parte dos interessados, das condições nele estabelecidas.

3. DAS CONDIÇÕES DE PARTICIPAÇÃO

3.1. Poderão participar deste Pregão os interessados que tenham o ramo de atividade compatível com o objeto desta licitação, atendam a todas as exigências deste Edital e seus anexos e que estejam devidamente cadastrados no Sistema **Licitações-e** do **Banco Brasil**, provedor do sistema eletrônico, por meio do sítio www.licitacoes-e.com.br, para acesso ao sistema eletrônico.

3.2. Caberá ao licitante interessado em participar do pregão eletrônico:

3.2.1. Credenciar-se no Sistema Licitações-e;

3.2.2. Remeter, exclusivamente por meio eletrônico, via internet, a proposta de preços;

3.2.3. Responsabilizar-se formalmente pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao provedor do sistema ou à EMAP responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros;

3.2.4. Acompanhar as operações no sistema eletrônico durante o processo licitatório, responsabilizando-se pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão;

3.2.5. Comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a viabilidade do uso da senha, para imediato bloqueio de acesso;

3.2.6. Utilizar-se de chave de identificação e da senha de acesso para participar do pregão na forma eletrônica.

3.3. A participação no pregão eletrônico dar-se-á pela utilização da senha privativa do licitante.

3.4. Não poderá participar direta ou indiretamente desta licitação, ou da execução do contrato, a empresa:

a) cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da Empresa Maranhense de Administração Portuária - EMAP;
b) que esteja cumprindo penalidade de suspensão aplicada pela Empresa Maranhense de Administração Portuária - EMAP;
c) declarada inidônea pela União, por Estado, pelo Distrito Federal ou por Município, enquanto perdurarem os efeitos da sanção;
d) constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;
e) constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;
f) cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;
g) que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea;
h) cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea.
i) Empresas em regime de consórcio, qualquer que seja sua forma de constituição.

3.5. Aplica-se a vedação prevista no subitem anterior:

a) à contratação do próprio empregado ou dirigente, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;
b) a quem tenha relação de parentesco, até o terceiro grau civil, com:
   i. dirigente da Empresa Maranhense de Administração Portuária;
   ii. empregado da Empresa Maranhense de Administração Portuária cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;
   iii. autoridade do ente público a que a Empresa Maranhense de Administração Portuária esteja vinculada;
   iv. cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a Empresa Maranhense de Administração Portuária há menos de 6 (seis) meses.

3.6. A participação no procedimento licitatório importa aceitação do Regulamento Interno da EMAP e do Código de Conduta da EMAP.

4. DA REPRESENTAÇÃO E DO CREDENCIAMENTO

4.1. Para acesso ao sistema eletrônico, os interessados em participar do Pregão deverão dispor de chave de identificação e senha pessoal (intransferíveis), obtidas junto às Agências do Banco do Brasil S.A., sediadas no País.

4.2. A chave de identificação e a senha poderão ser utilizadas em qualquer Pregão Eletrônico, salvo quando cancelada por solicitação do credenciado ou por iniciativa do Banco do Brasil, devidamente justificada.

4.3. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante.

4.4. O credenciamento do fornecedor e de seu representante, junto ao sistema eletrônico, implica na responsabilidade legal pelos atos praticados e a capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

4.5. A participação no Pregão Eletrônico dar-se-á por meio de digitação da chave e senha, pessoal e intransferível, do representante credenciado e subsequente encaminhamento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados a data e o horário limite estabelecidos.

4.6. A informação dos dados para acesso deve ser feita na página inicial do site www.licitacoes-e.com.br, opção "Acesso Identificado" e para acessar a sala de disputa a opção é "Sala de Disputa – acesse aqui".

4.7. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou à Empresa Maranhense de Administração Portuária - EMAP responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

5. DO ENVIO DA PROPOSTA DE PREÇOS

5.1. A licitante deverá encaminhar a proposta por meio do sistema eletrônico até a data e horário marcado para abertura da sessão, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.

5.2. Terá sua proposta desclassificada antes da disputa de lances a licitante que ao encaminhar a proposta, utilize campos textuais ou anexos para registrar ou inserir qualquer informação que venha a identificar sua razão social ou nome fantasia; ou efetue qualquer outro tipo de ação que permita sua identificação.

5.3. A licitante deverá registrar, na forma expressa no sistema eletrônico, o valor global da proposta, já inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.

5.4. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, caso o previsto não seja satisfatório para o atendimento do objeto da licitação.

5.5. A **Proposta de Preços readequada ao valor do lance final** deverá ser preenchida pela licitante em uma via, em papel timbrado da Empresa, em língua portuguesa, salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, assinada e rubricadas todas as folhas pelo representante legal da licitante proponente, devendo conter, obrigatoriamente, os elementos e informações seguintes:

a) **Número do Pregão e o nome ou razão social da licitante, número do CNPJ/MF, endereço completo, telefone, fax e endereço eletrônico (e-mail)**, este último se houver, para contato, bem como dados bancários (nome e número do Banco, agência e conta corrente para fins de pagamento);
b) **Termo de Compromisso de Cumprimento da Legislação Trabalhista, Previdenciária e de Segurança e Saúde do Trabalho**, podendo ser utilizado modelo constante do **Anexo III**, ou modelo próprio da licitante desde que contenha todas as informações solicitadas;
c) **Planilha de preços**, expressos em Reais (R$), com base no quantitativo de todos os itens do **Anexo II** (Modelo de Proposta) deste Edital, compreendendo a descrição do produto, unidade de medida, quantidade, o valor de cada item, valor total por item e valor total global, já incluídos na composição dos valores, todos os itens de despesas suportados pela licitante e tributos

porventura existentes, seja qual for o título ou a natureza (mão-de-obra, honorário, equipamentos, alimentação, transporte, passagem, hospedagem, EPI's, materiais, serviços, impostos, taxas, fretes, encargos sociais, locais, comerciais, trabalhistas e tudo mais que possa influenciar no custo final do objeto da licitação);

d) **Valor total da proposta** expresso em reais (R$), em algarismo e por extenso, permitidas apenas duas casas decimais após a vírgula;
e) **Prazo de validade da proposta** não inferior a 90 (noventa) dias, a contar da data de abertura da sessão pública do Pregão;
f) **Prazo de execução** será de 12 (doze) meses, a contar da data indicada na Ordem de Fornecimento (OF).

5.6 Caso algumas das informações descritas na alínea "a" não constem na proposta, poderão ser encaminhadas posteriormente até a data de assinatura do Contrato.

5.7 Havendo omissão do prazo de validade da proposta e/ou prazo de execução dos serviços na Proposta de Preços, a licitante não será desclassificada e o Pregoeiro entenderá como sendo iguais aos previstos nas alíneas "e" e "f" do subitem acima.

5.8 Quaisquer tributos, custos e despesas diretos ou indiretos omitidos da proposta ou incorretamente cotados, serão considerados como inclusos nos preços, não sendo considerados pleitos de acréscimos, a esse ou qualquer título, devendo os serviços serem executados sem quaisquer ônus adicionais para a EMAP.

5.9 Não serão consideradas as propostas com alternativas não previstas neste instrumento, devendo as licitantes se limitar às especificações deste Edital e do Termo de Referência.

6. DA FORMULAÇÃO DOS LANCES

6.1 Aberta a etapa competitiva (Sessão Pública de Lances), no horário previsto no preâmbulo, os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.

6.2 Os licitantes poderão oferecer lances sucessivos, observando o horário fixado e as regras de aceitação dos mesmos.

6.3 Somente serão aceitos os lances cujos valores forem inferiores ao último lance que tenha sido anteriormente ofertado pelo licitante.

6.4 Não serão aceitos dois ou mais lances iguais, prevalecendo aquele que for recebido e registrado primeiro pelo sistema.

6.5 Durante a Sessão Pública da Licitação Eletrônica, os licitantes serão informados em tempo real, do valor do menor lance registrado, vedada a identificação do seu detentor.

6.6 A etapa de lances será encerrada mediante aviso de seu fechamento iminente aos licitantes, por meio do Sistema Eletrônico.

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

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

6.9 Se a desconexão perdurar por tempo superior a 10 (dez) minutos, a sessão será suspensa e terá reinício somente após comunicação expressa do Pregoeiro aos participantes.

6.10 A etapa de lances da sessão pública será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico aos licitantes, após o que transcorrerá um período de tempo aleatório de até 30 (trinta) minutos, durante o qual, a qualquer momento, o sistema encerrará automaticamente a recepção de lances.

6.11 Encerrada a etapa de lances da sessão pública e definida a melhor proposta, o Pregoeiro poderá negociar, via sistema eletrônico, para que seja obtida melhor proposta. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7 DO JULGAMENTO DAS PROPOSTAS

7.1 No julgamento das propostas, a classificação se dará em ordem crescente dos preços apresentados, sendo considerada vencedora a proposta mais vantajosa, observados os prazos, as especificações técnicas, os parâmetros mínimos de desempenho e de qualidade e as demais condições definidas neste Edital e seus anexos.

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

7.3 O preço aceitável deverá ser igual ou inferior ao orçamento total estimado.

7.4 Serão desclassificadas as Propostas de Preços que:

7.4.1 Não atenderem às exigências do presente Edital e seus Anexos.

7.4.2 Contenha vícios insanáveis.

7.4.3 Descumpra especificações técnicas constantes deste instrumento convocatório.

7.4.4 Apresente preços manifestamente inexequíveis.

7.4.4.1 Caso entenda que o preço é inexequível, deverá antes de desclassificar a proposta, estabelecer prazo para que o licitante demonstre a exequibilidade de seu preço.

7.4.5 Não tenha sua exequibilidade demonstrada, quando exigida.

7.4.6 Não estiver acompanhada do Termo de Compromisso de Cumprimento da Legislação Trabalhista, Previdenciária e de Saúde e Medicina do Trabalho ou não conter o citado Termo;

7.4.7 Apresentar, após a fase de lance ou negociação, preço total acima do orçamento estimado;

7.4.8 Apresentar prazo de validade da proposta e/ou prazo de execução em desacordo com o estabelecido neste Edital;

7.4.9 Apresentar proposta de preço com qualquer item com especificação e/ou quantitativos divergentes dos previstos no Anexo II – Modelo de Proposta, deste Edital, que venha a comprometer significativamente o objetivo final da contratação;

7.4.10 Não enviar a proposta ajustada ao lance e a documentação solicitada e/ou enviá-las fora do prazo estabelecido;

7.4.11 Deixar de apresentar preço para qualquer item constante do Anexo II - Modelo de Proposta deste Edital;

7.4.12 Forem apresentadas com rasuras, emendas, borrões ou entrelinhas de modo a ensejar dubiedade, principalmente em relação a valores.

7.5 Se a proposta ou o lance de menor preço não for aceitável, ou se a licitante desatender às exigências habilitatórias, o Pregoeiro examinará a proposta ou o lance subsequente, verificando a sua aceitabilidade e procedendo à sua habilitação, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda ao edital.

7.6 Encerrada a etapa de lances, o sistema identificará as microempresas, empresas de pequeno porte e microempreendedor individual - MEI, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, sendo consideradas empatadas, as propostas de microempresas, empresas de pequeno porte e MEI que se encontrarem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço.

7.6.1 Aplica-se o disposto no subitem anterior somente no caso da proposta inicialmente mais bem classificada não ter sido apresentada por microempresa, empresa de pequeno porte e microempreendedor individual – MEI.

7.6.2 A microempresa, empresa de pequeno porte e microempreendedor individual - MEI considerada empatada e mais bem classificada será convocada, após o término de lances, para apresentar nova proposta de preço inferior àquela considerada vencedora do certame em até 5 (cinco) minutos da convocação, sob pena de preclusão.

7.6.3 A microempresa, empresa de pequeno porte e microempreendedor individual - MEI acima indicada que efetivamente apresente nova proposta de preço inferior àquela considerada vencedora do certame, desde que em tempo hábil, terá adjudicado em seu favor o objeto licitado.

7.6.4 Caso a microempresa, empresa de pequeno porte e microempreendedor individual - MEI mais bem classificada não apresente proposta mais vantajosa (Menor Preço) àquela inicialmente vencedora, serão convocadas as demais remanescentes consideradas empatadas na ordem classificatória, para o exercício do direito de ofertar proposta de preço inferior àquela considerada vencedora do certame.

7.6.5 No caso de equivalência dos valores apresentados por microempresa, empresa de pequeno porte e microempreendedor individual - MEI que se encontrem no intervalo estabelecido no caput deste subitem, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta, conforme disposto no inciso III, art. 45 da Lei Complementar n° 123/2006.

7.7 CRITÉRIO DE DESEMPATE

7.7.1 Em caso de empate entre propostas na primeira colocação, o Pregoeiro adotará os seguintes critérios de desempate, nesta ordem:

7.7.1.1 Disputa final, em que os licitantes empatados poderão apresentar nova proposta fechada, no sistema, em ato contínuo ao encerramento da etapa de julgamento;

7.7.1.2 Os critérios estabelecidos no artigo 3º da Lei nº 8.248, de 23 de outubro de 1991 (Lei de Informática e Automação), e no artigo 118 do Regulamento de Licitações e Contratos da Empresa Maranhense de Administração Portuária – EMAP;

7.7.1.3 Sorteio.

7.7.2 Entende-se por empate aquelas situações em que as propostas apresentadas, atendidas todas as condições estipuladas neste Edital, contenham valores exatamente iguais.

7.7.3 A disputa final será realizada em ato contínuo ao encerramento da sessão de disputa de lances entre os licitantes empatados em primeiro lugar.

7.7.3.1 Os licitantes que se encontrem na situação de empate poderão, no prazo decadencial de 10 (dez) minutos, apresentar um novo lance fechado por meio da opção "Enviar Lances de Desempates", disponível no resumo do lote da licitação, fora da sala de disputa do licitações-e.

7.7.4 Para fins de classificação final, será sempre considerado o menor lance dentre os apresentados pelo licitante, incluindo eventual lance de desempate.

7.7.5 Caso persista o empate após a aplicação de todos os critérios anteriores ao sorteio, este último será realizado em ato público, mediante comunicação formal do dia, hora e local, feita com antecedência mínima de 3 (três) dias úteis, no próprio ambiente eletrônico da licitação, no Chat de Mensagens do lote.

7.7.5.1 Decorridos 30 (trinta) minutos da hora marcada, sem que compareçam os interessados, o sorteio será realizado a despeito das ausências.

7.7.6 Em caso de empate nas demais colocações, será observada a ordem cronológica dos lances, tendo prioridade, em eventual convocação, o licitante cujo lance tenha sido recebido e registrado antes.

8 DA HABILITAÇÃO

8.1 Após as fases de lances e análise e aceitabilidade da proposta de preço, o pregoeiro analisará a documentação de habilitação do licitante que apresentou a proposta mais vantajosa, segundo os critérios de julgamento fixados no instrumento convocatório.

8.2 Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

8.2.1 SICAF;
8.2.2 Cadastro Nacional de Empresas Inidôneas - CEIS;
8.2.3 Cadastro Nacional de Empresas Punidas – CNEP;
8.2.4 Lista de fornecedores sancionados do Portal SIGA-MA;
8.2.5 CNCIA – Cadastro Nacional de Condenados por Ato de Improbidade Administrativa.

8.3 Para fins de habilitação a licitante classificada detentora da proposta mais vantajosa deverá apresentar os seguintes documentos:

a) Habilitação Jurídica;

b) Regularidade Fiscal e Trabalhista;
c) Qualificação Econômica e Financeira;
d) Qualificação Técnica e/ou Operacional;
e) Outros Documentos.

8.4 A **HABILITAÇÃO JURÍDICA** deverá ser comprovada por meio da apresentação da seguinte documentação:

8.4.1 **Registro Comercial**, no caso de empresa individual;

8.4.2 **Ato constitutivo**, **Estatuto** ou Contrato Social em vigor, devidamente atualizado e registrado, em se tratando de sociedades empresariais e, no caso de sociedades por ações, acompanhados dos documentos de eleição de seus atuais administradores. Estes documentos deverão estar acompanhados de todas as alterações, ou de documentos consolidados, se houver, devidamente registrados na Junta Comercial ou em órgão equivalente;

8.4.3 **Inscrição do ato constitutivo**, no caso de sociedades civis, acompanhado de prova da diretoria em exercício;

8.4.4 **Decreto de autorização**, em se tratando de empresa ou sociedade estrangeira em funcionamento no país, e ato de registro ou autorização para funcionamento, expedido pelo órgão competente, quando a atividade assim o exigir.

8.5 A **REGULARIDADE FISCAL** e **TRABALHISTA** deverá ser comprovada por meio da apresentação dos seguintes documentos:

8.5.1 **Prova de regularidade fiscal perante a Fazenda Federal**, efetuada mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), incluindo os créditos tributários relativos às contribuições sociais previstas nas alíneas "a", "b" e "c" do parágrafo único do art. 11 da Lei nº 8.212/91 (INSS), nos termos da Portaria Conjunta PGFN/RFB Nº 1.751, de 02.10.2014.

8.5.2 **Prova de regularidade com a Fazenda Estadual** do domicílio ou sede do licitante, mediante apresentação das seguintes certidões:

8.5.2.1 Certidão Negativa de Débitos Fiscais (não inscritos na Dívida Ativa), e;

8.5.2.2 Certidão Negativa de Inscrição de Débitos na Dívida Ativa;

8.5.2.3 Quando a prova de regularidade de que trata este subitem for comprovada mediante a apresentação de uma única certidão, e dela não constar expressamente essa informação, caberá a licitante demonstrar com documentação hábil essa condição.

8.5.3 **Prova de regularidade com a Fazenda Municipal** do domicílio ou sede do licitante, emitida até 90 (noventa) dias contados da data de entrega dos envelopes, relativa ao ISSQN – Imposto Sobre Serviços de Qualquer Natureza e relativa à TLF – Taxa de Localização e Funcionamento, mediante apresentação das seguintes certidões:

8.5.3.1 Certidão Negativa de Débitos Municipais (não inscritos na Dívida Ativa), e;

8.5.3.2 Certidão Negativa quanto à Divida Ativa Municipal;

8.5.3.3 Quando a prova de regularidade de que trata este subitem for comprovada mediante a apresentação de uma única certidão, e dela não constar expressamente essa informação,

caberá a licitante demonstrar com documentação hábil essa condição, sendo que para as empresas estabelecidas no município de São Luís-MA., a prova de regularidade deverá ser feita mediante a apresentação da **Certidão Negativa de Débitos**, conforme Instrução Normativa n.º 04/2016-GS-SEMFAZ.

8.5.4 Prova de Regularidade relativa ao **Fundo de Garantia por Tempo de Serviço – FGTS**.

8.5.5 **Certidão Negativa de Débitos Trabalhistas** – CNDT, conforme Lei nº 12.440/2011.

8.5.6 As microempresas, empresas de pequeno porte e microempreendedores individuais deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal e trabalhista relacionadas no item 8.5 deste edital, mesmo que esta apresente alguma restrição, assegurado, todavia, o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada vencedora do certame, prorrogáveis por igual período, a critério do Pregoeiro, ou diretamente 10 (dez) dias úteis, a critério do Pregoeiro, para reapresentação da documentação devidamente regularizada.

8.5.7 A não regularização da documentação, no prazo previsto no subitem anterior, implicará na decadência do direito à contratação e a licitante será considerada inabilitada, cabendo à Administração selecionar a oferta subsequente em ordem de preço, verificando se existem outros licitantes com direito de preferência no mesmo intervalo, quando for o caso, e proceder ao exame de conformidade da proposta, a sua aceitabilidade e a habilitação da licitante, e assim sucessivamente até encontrar uma que atenda aos requisitos do Edital e aos interesses da EMAP.

8.6 A **QUALIFICAÇÃO ECONÔMICO-FINANCEIRA** será comprovada mediante a apresentação dos seguintes documentos:

8.6.1 Balanço Patrimonial e Demonstração de Resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais (2022 e 2023), vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 03 (três) meses da data de apresentação da proposta, que comprove a boa situação financeira da empresa baseada nas condições seguintes:

a) A comprovação de boa situação financeira da empresa licitante será demonstrada através de índice financeiro utilizando-se as fórmulas abaixo, cujos resultados deverão estar de acordo com os valores estabelecidos:

b)

a.1) **Índice de Liquidez Geral (ILG)**

$$ILG = \frac{\text{Ativo Circulante + Ativo Não Circulante}}{\text{Passivo Circulante + Passivo Não Circulante}} \geq 1{,}0$$

b.2) **Índice de Liquidez Corrente (ILC)**

$$ILC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}} \geq 1{,}0$$

c) As empresas que apresentarem quaisquer dos índices relativos à boa situação financeira

menor do que o exigido, quando de sua habilitação, deverão comprovar, considerados os riscos para a administração, Capital Social ou Patrimônio Líquido no valor mínimo de 10% (dez por cento) do valor inicial da sua proposta;

d) Os índices contábeis apurados na análise do balanço patrimonial deverão ser informados pela licitante, conforme as fórmulas acima indicadas, expressando os valores em Reais dos grupos de contas envolvidos. Caso o memorial não seja apresentado, a Comissão reserva-se no direito de efetuar os cálculos.

8.6.1.1 As empresas com menos de um exercício financeiro devem cumprir a exigência deste item mediante a apresentação do Balanço de Abertura, o qual deverá constar elementos que comprovem a boa situação financeira da mesma.

8.6.1.2 Serão considerados aceitos como na forma da lei o balanço patrimonial e demonstrações contábeis assim apresentados:

a) Publicados em Diário Oficial ou
b) Publicados em jornal de grande circulação ou;
c) Registrados na Junta Comercial da sede ou domicílio do licitante ou;
d) Por cópia do Livro Diário, devidamente autenticado na Junta Comercial da sede ou domicílio da empresa, na forma da Instrução Normativa nº 11, de 05 de dezembro de 2013, do Departamento de Registro Empresarial e Integração-DREI, acompanhada obrigatoriamente dos Termos de Abertura e de Encerramento.

8.6.1.3 Ocorrendo alteração do Capital Social após a realização do Balanço Patrimonial, a licitante deverá apresentar documentação que comprove essa alteração, devidamente registrada na Junta Comercial, incluindo, no caso de empresas estabelecidas no Estado do Maranhão, apresentação de Certidão atualizada da Jucema (Decreto Estadual nº 21.040/05).

8.6.1.4 A pessoa jurídica optante do Sistema de Lucro Real ou Presumido, somente a que distribuem lucro, deverá apresentar juntamente com o Balanço Patrimonial, cópia do recibo de entrega da escrituração contábil digital – SPED CONTÁBIL, nos termos da IN RFB 1.420/2013, 1.422/2013, IN RFB 1.486/2014, IN RFB 1.510/2014, IN RFB 1.594/2015 e IN RFB 1.660/2016.

8.6.2 **Certidão Negativa de Falência**, expedida pelo distribuidor da sede da pessoa jurídica, com data não excedente a 60 (sessenta) dias de antecedência da data de apresentação da proposta de preço e dos documentos de habilitação, quando não vier expresso o prazo de validade.

8.7 A **QUALIFICAÇÃO TÉCNICA** deverá ser comprovada por meio da apresentação dos documentos indicados no item 11 do Termo de Referência (Anexo I).

8.8 **OUTROS DOCUMENTOS:**

8.8.1 **Certidão Simplificada da Junta Comercial do Estado do Maranhão (JUCEMA)**, comprobatória da situação atualizada do seu registro, ato constitutivo, estatuto ou contrato social em vigor, em cumprimento aos termos do art. 1º do Decreto Estadual nº 21.040/2005, **exigível somente para empresários e sociedades empresariais do Estado do Maranhão**. O Microempreendedor Individual-MEI, em razão do seu tipo jurídico e de seu procedimento de registro, alteração, baixa e legalização ser realizado pelo Portal do Empreendedor, no qual expressa a sua situação cadastral com o número do registro e CNPJ, considerados certidões, está dispensado de apresentar a certidão da JUCEMA.

8.8.2 Declaração de que não emprega menores de dezoito anos em trabalho noturno, perigoso ou insalubre e nem menores de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz, a partir de quatorze anos, de conformidade com o disposto no art. 7º, inciso XXXIII da Constituição Federal, nos termos do Anexo V.

8.9 O licitante que possuir habilitação parcial atualizada no Sistema de Cadastramento Unificado de Fornecedores – SICAF, Registro Cadastral Oficial do Poder Executivo Federal, ficará isento de apresentar os documentos relacionados nos subitens Registro Comercial, Ato constitutivo, Contrato Social ou Estatuto, acompanhado dos documentos de eleição de seus atuais administradores, em se tratando de sociedade por ações, Inscrição do ato constitutivo, regularidade fiscal e trabalhista e Balanço Patrimonial e Demonstrações Contábeis, nos termos do item **DA HABILITAÇÃO**. A verificação da habilitação junto ao SICAF, será feita "on-line'". Caso algum dos documentos citados anteriormente não constem do SICAF, a licitante deverá encaminhá-lo no prazo de até 04 (quatro) horas, a contar da convocação do Sistema (Licitações-e).

8.10 Todos os documentos deverão estar em nome da licitante. Se a licitante for matriz, os documentos deverão estar com o número do CNPJ da matriz. Se for filial, os documentos deverão estar com o número do CNPJ da filial, salvo aqueles que, por sua natureza, comprovadamente, são emitidos em nome da matriz.

8.11 Não serão aceitos protocolos de entrega ou solicitação de documentos em substituição aos documentos requeridos no presente Edital e seus Anexos.

8.12 Se a documentação de habilitação não estiver completa e correta ou contrariar qualquer dispositivo deste Edital e seus Anexos, poderá o Pregoeiro considerar o proponente inabilitado.

8.13 A declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte sujeitará a licitante às sanções previstas neste edital.

9 DO ENCAMINHAMENTO DA DOCUMENTAÇÃO E DA PROPOSTA

9.1 Após a etapa de negociação, a licitante detentora do menor lance deverá encaminhar sua **Proposta de Preços**, nos termos do item DO ENVIO DA PROPOSTA DE PREÇO, preenchida com os valores unitários e total, atualizados em conformidade com o menor lance ofertado e **de acordo com o Anexo II**, e demais **documentos exigidos para habilitação** que não estiverem disponíveis no **SICAF**, **no prazo máximo de até 04 (quatro) horas**, a contar da convocação do Pregoeiro no Sistema (Licitações-e), por meio do menu "opções" e depois "incluir anexo proposta" no sistema Licitações-e ou por meio do endereço eletrônico csl@emap.ma.gov.br. **Em vista a capacidade do sistema é importante compactar o arquivo para até 20MB.**

9.2 Após análise, a proposta ajustada e os documentos de habilitação deverão ser encaminhados em originais ou cópias autenticadas, por meio de Cartório competente, **no prazo de até 05 (cinco) dias úteis**, contados da data da solicitação do Pregoeiro, ao endereço da EMAP, na Avenida dos Portugueses, Porto do Itaqui, s/n, Bairro Itaqui, CEP 65.085-370, São Luís – MA**.**

9.2.1 Em homenagem à razoável duração dos processos (art. 5º, LXXVIII, CF/88), caso, em atendimento ao disposto no item 9.1, toda a proposta ajustada e todos os documentos de habilitação enviados à CSL/EMAP tenham sido assinados digitalmente, com a indicação do

endereço eletrônico para reconhecimento da assinatura digital e/ou confirmação eletrônica de autenticidade, a licitante detentora da menor proposta ficará dispensada da remessa da documentação em original ou em cópia autenticada.

9.3 O não envio dos documentos ou o envio em desacordo com o Edital ou o decurso do prazo mencionado nos subitens anteriores ensejará a recusa da proposta.

10 DOS RECURSOS

10.1 Dos atos do pregoeiro neste processo licitatório, poderá o licitante, na forma do art. 129 do Regulamento de Licitações e Contratos da EMAP, ao final da Sessão Pública manifestar, imediata e motivadamente, a intenção de interpor recurso.

10.2 Declarado o vencedor, qualquer Licitante poderá manifestar imediata e motivadamente a intenção de recorrer, quando lhe será concedido o prazo de **05 (cinco) dias úteis**, contado a partir da intimação do ato de julgamento da habilitação, para apresentação das razões do recurso, devendo contemplar, conforme o caso, além dos atos praticados na fase de habilitação, aqueles praticados em decorrência do julgamento das propostas e da verificação da efetividade dos lances ou propostas, ficando os demais Licitantes desde logo intimados para apresentar impugnações em igual prazo, que começarão a correr do término do prazo do recorrente, sendo-lhes assegurada vista dos autos.

10.3 A falta de manifestação recursal do licitante, dentro do prazo de 30 (trinta) minutos, **após declarado o vencedor da licitação**, importará na decadência do direito de recurso e a Adjudicação do objeto da licitação pelo Pregoeiro ao vencedor.

10.4 As razões do recurso bem como as contrarrazões deverão ser encaminhadas por meio do endereço eletrônico csl@emap.ma.gov.br ou protocolizados no Setor de Protocolo da EMAP, localizado no Prédio sede da EMAP, na Avenida dos Portugueses, s/n, Itaqui, São Luís-MA, dentro do horário de expediente da EMAP, das 08:00 às 12:00 e das 13:00 às 17:00 horas.

10.5 O recurso contra a decisão do Pregoeiro terá efeito suspensivo e, se acolhido, invalidará apenas os atos insuscetíveis de aproveitamento.

10.6 Os autos do processo permanecerão com vista franqueada aos interessados, na EMAP, no Porto do Itaqui, s/n, Itaqui – São Luís/MA, durante os dias úteis, das 08:00 às 12:00 horas e das 13:00 às 17:00 horas.

10.7 Se não reconsiderar sua decisão, o Pregoeiro submeterá o recurso, devidamente informado, à consideração do Presidente da EMAP, que proferirá decisão definitiva antes da homologação do procedimento, no prazo de até 05 (cinco) dias úteis, contado de seu recebimento.

11 DA HOMOLOGAÇÃO E CONTRATAÇÃO

11.1 O resultado de julgamento será submetido à Autoridade Competente para homologação.

11.2 Após a homologação do resultado da presente licitação pelo Presidente da EMAP, a empresa adjudicatária será convocada, por meio de correspondência específica, para no prazo máximo de até **10 (dez) dias corridos**, contados da data do ofício de convocação, assinar o Contrato, e entregar o **Questionário de Diligências Prévias** (**Anexo VI**) devidamente preenchido, sob pena de decair o direito da contratação, sem prejuízo das sanções previstas neste Edital.

11.2.1 A assinatura do contrato poderá ser realizada na sede da EMAP; eletronicamente (utilizando-se de certificado digital, disponibilizado pela ICP-Brasil - certificado digital emitido por uma Autoridade Certificadora (AC) credenciada na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na forma da legislação vigente); ou na forma do subitem 11.2.2 deste edital.

11.2.2 Observado o prazo indicado no subitem 11.2, a empresa adjudicatária procederá à impressão colorida e integral de 03 (três) vias do contrato e dos respectivos anexos e coletará a assinatura dos respectivos representantes legais. Competir-lhe-á, ainda, reconhecer em cartório a firma do respectivo signatário do instrumento contratual e da respectiva testemunha, remetendo, nas vinte e quatro horas seguintes a esse reconhecimento, por companhia aérea, as três vias do termo contratual e de eventual documentação requerida no ato de convocação.

11.3 O prazo da convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela licitante vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela EMAP.

11.4 A recusa injustificada da licitante vencedora em assinar o Contrato, prestar a garantia, se houver, e receber a Ordem de Serviço/Fornecimento, dentro do prazo estabelecido pela EMAP, caracteriza o descumprimento total da obrigação assumida, sujeitando-a as penalidades legalmente estabelecidas.

11.5 No ato da assinatura do contrato, caso a adjudicatária tenha sede ou filial estabelecida no Estado do Maranhão deverá apresentar comprovação de regularidade com a CAEMA, consoante determina o Decreto Estadual nº 21.178, de 26 de abril de 2005.

11.6 A contratação fica condicionada à confirmação da autenticidade das certidões sujeitas à confirmação e à consulta prévia pela EMAP ao Cadastro Estadual de Inadimplentes - CEI, consoante determina o art. 6º da Lei Estadual nº 6.690, de 11 de julho de 1996 (regulamentado pelo Decreto n.º 21.331, de 20 de julho de 2005).

11.7 A contratação fica condicionada à consulta prévia pela EMAP ao Cadastro de Empregadores que tenham submetido trabalhadores a condições análogas à de escravo divulgada no sítio eletrônico do Ministério do Trabalho e Emprego, consoante determina a Lei Estadual nº 9.752, de 10 de janeiro de 2013.

12 DAS SANÇÕES ADMINISTRATIVAS

12.1 A licitante que ensejar o retardamento da execução do certame, não mantiver a sua proposta, tumultuar a sessão, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito prévio da citação e da ampla defesa, ficará impedido de licitar a contratar com a EMAP, pelo prazo de 02 dois anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a sua reabilitação perante a própria EMAP.

12.2 O Contratado cometerá infração administrativa se:

12.2.1 apresentar documentação falsa;

12.2.2 retardar a execução do objeto;

12.2.3 falhar na execução contratual;

12.2.4 fraudar na execução contratual;

12.2.5 comportar-se de modo inidôneo;

12.2.6 não mantiver a proposta;

12.2.7 inexecutar, total ou parcialmente, qualquer das obrigações assumidas em decorrência da contratação;

12.2.8 fizer declaração falsa.
12.2.9 cometer fraude fiscal
12.3. Observada a ampla defesa, o Contratado que cometer qualquer das infrações discriminadas acima ficará sujeito, sem prejuízo da responsabilidade civil e criminal e da rescisão unilateral do contrato, às seguintes sanções:
12.3.1 advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;
12.3.2 multa moratória, pelo atraso injustificado na execução contratual, configurado mediante o retardamento dessa execução, ou a falha na execução contratual, ou, ainda, a inexecução parcial de qualquer das obrigações assumidas em decorrência da contratação;
12.3.3 multa compensatória, pela apresentação de documentação falsa, pela falha na execução contratual, pela fraude na execução contratual, pelo comportamento de modo inidôneo, pela não manutenção da proposta, pela inexecução total da obrigação assumida em decorrência da contratação e pela prestação de declaração falsa;
12.3.4 suspensão temporária de participação em licitação e impedimento de contratar com a Contratante, por prazo não superior a 2 (dois) anos.
12.4. As sanções decorrentes da inexecução total ou parcial de quaisquer das obrigações contratualmente assumidas e de comportamento inidôneo poderão ser aplicadas juntamente com a multa compensatória, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis.
12.4.1 A aplicação da multa moratória não impede que a Contratante rescinda o contrato e aplique as outras sanções previstas neste edital e será aplicada após regular processo administrativo, podendo ser descontada da garantia do respectivo contratado, se houver.
12.4.1.1 Se a multa moratória for de valor superior ao valor da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Contratante ou, ainda, quando for o caso, cobrada judicialmente.
12.5 Reputar-se-ão inidôneos atos tais como os descritos nos artigos 337-F, 337-L e 337-M, §2º do Código Penal.
12.6 A multa moratória será calculada sobre o percentual de 1% (um por cento) do valor unitário do bem em atraso, por dia, por unidade, até o limite de 20% (vinte por cento) do valor do contrato.
12.6.1. Considera-se inexecução parcial o atraso injustificado no prazo de entrega até o limite de 10 (dez) dias.
12.7 A multa compensatória será de, no máximo, 30% (trinta por cento) do valor do contrato.
12.7.1 Considera-se inexecução total o atraso injustificado no prazo de entrega superior a 10 (dez) dias.
12.7.2 O não-cumprimento de obrigação contratual acessória, a exemplo de eventual garantia exigida para os produtos, sujeitará o Contratado à multa de até 10% (dez por cento) do valor do contrato.
12.8. O valor da multa poderá ser descontado das faturas devidas ao Contratado.
12.8.1 O valor da multa também poderá ser descontado da garantia de execução contratual, se houver.
12.8.2 Se os valores das faturas ou da garantia de execução contratual forem insuficientes, fica o Contratado obrigado a recolher a importância devida no prazo de 15 (quinze) dias, contados da comunicação oficial.
12.8.3 Esgotados os meios administrativos para a cobrança do valor devido pelo Contratado à Contratante, o débito será cobrado judicialmente.

12.9 O contratado sujeita-se à suspensão temporária de participação em licitação e ao impedimento de contratar com a Contratante:
12.9.1 pelo prazo de 2 (dois) anos, quando apresentar documentação falsa, fraudar a execução contratual, comportar-se de modo inidôneo ou fizer declaração falsa;
12.9.2 por prazo não superior a 2 (dois) anos, quando retardar a execução do objeto, falhar na execução do objeto, inexecutar o objeto contratual ou não mantiver a proposta.
12.9.3 As sanções previstas nos subitens anteriores poderão ser aplicada às empresas ou aos profissionais que, em razão deste contrato:
12.9.3.1. tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
12.9.3.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
12.9.3.3. demonstrem não possuir idoneidade para contratar com a Empresa Maranhense de Administração Portuária em virtude de atos ilícitos praticados.
12.10. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto na Lei nº 13.303/2016, no Regulamento de Licitações e Contratos da EMAP e, subsidiariamente, na Lei Estadual nº 8.959/2009.

12.10.1 A aplicação da penalidade pelo descumprimento das exigências de implantação do Programa de Integridade previstas na Lei Ordinária nº 11.463, de 04 de maio de 2021, realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto na referida Lei.
12.11 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

12.12 A Contratante informará os dados relativos às sanções por ela aplicadas aos contratados, nos termos definidos nos arts. 37 e 83 da Lei nº 13.303/2016, de forma a manter atualizado o cadastro de empresas inidôneas de que trata o art. 23 da Lei no 12.846/2013.

13 DA DOTAÇÃO ORÇAMENTÁRIA

13.1 As despesas decorrentes dos serviços, objeto desta contratação, correrão por conta da disponibilidade financeira e orçamentária no Orçamento Geral da EMAP, fonte 227 – recursos das empresas estatais – exercício financeiro – 2024 – CAPEX TI - Aquisição de 2 aplliances de Firewall e XDR.

14 DA GARANTIA DE EXECUÇÃO DO CONTRATO

14.1 A Contratada prestará garantia, em até 10 (dez) dias úteis após a assinatura do contrato, no percentual de 5% (cinco por cento) do valor global contratado, observado as indicações do Termo de Referência e deste Edital, a qual se estenderá por 03 (três) meses após o término da vigência contratual, devendo ser renovada a cada prorrogação, em uma das modalidades a seguir, não sendo concedido, em nenhuma hipótese, prazo para apresentação da garantia após esse prazo:

14.1.1. caução em dinheiro;

14.1.2. seguro-garantia;

14.1.3. fiança bancária.

14.2. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

14.2.1. prejuízos advindos do não cumprimento do contrato;

14.2.2. multas aplicadas à Contratada;

14.2.3. prejuízos diretos causados à Contratante decorrentes de culpa ou de dolo durante a execução do contrato;

14.2.4. obrigações previdenciárias e trabalhistas não honradas pela Contratada.

14.3. Se a opção de garantia for a caução em dinheiro, a Contratada deverá solicitar informações à EMAP referentes ao nome da instituição financeira, aos números da conta corrente e da agência bancária, e ao código identificador, para efeito de depósito do crédito, sendo que o valor caucionado será restituído considerando-se os critérios vigentes de remuneração da poupança aplicados à época da devolução.

14.4. Se a opção recair em seguro-garantia, deverá ser feita a entrega da apólice em original, acompanhada de comprovante de pagamento do respectivo prêmio, devendo ainda conter expressamente cláusula de atualização financeira, de imprescritibilidade, inalienabilidade e de irrevogabilidade e deverá ser válida por pelo menos 90 (noventa) dias consecutivos após o prazo de validade deste contrato. A modalidade seguro garantia somente será aceita se contemplar todos os eventos indicados no parágrafo primeiro da cláusula décima deste Contrato.

14.5. Se a opção recair em fiança bancária, deverá ser feita a entrega da Carta de Fiança, em original, assinada pelo(s) representante(s) legal(is) do emitente devidamente comprovado, devendo conter expressamente cláusula de atualização financeira, de imprescritibilidade, inalienabilidade e de irrevogabilidade e deverá ser válida por pelo menos 90 (noventa) dias consecutivos após o prazo de validade do contrato.

14.6. Caso ocorra a prorrogação do Contrato, a Contratada fica obrigada a apresentar, no ato da assinatura do Termo Aditivo ou em até 10 (dez) dias dessa data, a critério da EMAP, a renovação da caução prestada quando a mesma tiver sido feita nas modalidades de seguro garantia ou fiança bancária.

14.7. A Contratante poderá descontar do valor da garantia toda e qualquer importância que lhe for devida, a qualquer título, pela Contratada, inclusive multas.

14.8. Se o desconto se efetivar no decorrer do prazo contratual, a caução deverá ser reintegrada no prazo de 05 (cinco) dias úteis, a contar da data de recebimento da notificação, sob pena de ser descontada na fatura seguinte.

14.9. A garantia será restituída após o cumprimento das obrigações contratuais, devidamente atestado pela Fiscalização e/ou Comissão da EMAP designada para esse fim.

15. DO PROGRAMA DE INTEGRIDADE

15.1. Nos termos do disposto na Lei Ordinária nº 11.463, de 04 de maio de 2021, fica estabelecida a exigência de programa de integridade às empresas que celebrarem contrato, consórcio, convênio, concessão ou parceria público-privada com a Empresa Maranhense de Administração Portuária-EMAP,

cujos limites anuais em valor sejam **superiores a R$ 8.000.000,00 (oito milhões de reais) para obras e serviços de engenharia e R$ 4.000.000,00 (quatro milhões de reais) para compras e serviços**, mesmo que na forma de pregão eletrônico, não se aplicando tal exigência às microempresas e empresas de pequeno porte, conforme a Lei Complementar Federal nº 155/2016.

15.2 No ato da assinatura do contrato, a adjudicatária deverá comprovar a existência de Programa de Integridade, que será avaliado de acordo com os parâmetros constantes no art. 5º da Lei Ordinária nº 11.463, de 04 de maio de 2021, devendo apresentar relatório de perfil e relatório de conformidade do Programa, conforme art. 6º da referida lei.

15.3 Na hipótese de inexistência de Programa de Integridade implantado no âmbito da empresa, a adjudicatária deverá implantar o Programa no prazo de 120 (cento e vinte) dias corridos, a partir da data de celebração do contrato.

15.4 Os custos e despesas com a implantação e manutenção do Programa de Integridade ficam a cargo da pessoa jurídica contratada, não cabendo à Empresa Maranhense de Administração Portuária-EMAP o seu ressarcimento

15.5 Pelo descumprimento das exigências referidas na Lei Ordinária nº 11.463, de 04 de maio de 2021, a Empresa Maranhense de Administração Portuária-EMAP poderá aplicar à pessoa jurídica contratada multa equivalente a 0,08%, por dia, incidente sobre o valor atualizado do contrato, limitado a 10% do valor atualizado do contrato.

16 DAS DISPOSIÇÕES GERAIS

16.1 O presente Edital e seus Anexos, bem como a proposta da licitante vencedora, farão parte integrante do Contrato, independentemente de transcrição.

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

16.3 Fica assegurado à Empresa Maranhense de Administração Portuária - EMAP o direito de no interesse da Administração, anular ou revogar, a qualquer tempo, no todo ou em parte, a presente licitação, dando ciência aos participantes, na forma da legislação vigente.

16.4 Os licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

16.5 Após a apresentação da proposta não caberá desistência, salvo por motivo justo, decorrente de fato superveniente e aceito pelo Pregoeiro.

16.6 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 e local anteriormente estabelecidos, desde que não haja comunicação do Pregoeiro em contrário.

16.7 Só se iniciam e vencem os prazos em dias de expediente na Empresa Maranhense de Administração Portuária - EMAP.

16.8 O desatendimento de exigências formais não essenciais não importará no afastamento da licitante, desde que sejam possíveis a aferição da sua qualificação e a exata compreensão da sua proposta, durante a realização da sessão pública do Pregão.

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

16.10 Envelopes e demais documentos não reclamados no prazo de 30 (trinta) dias, contados da data de homologação (ou, ainda, de revogação e/ou anulação do certame), serão destruídos, independentemente de notificação ao interessado.

16.11 O resultado desta licitação será comunicado no mesmo dia do julgamento, se proferido no dia da abertura, ou mediante publicação na Imprensa Oficial e/ou Jornal de grande circulação, e/ou no sítio da EMAP, e/ou mediante comunicação diretamente aos interessados.

16.12 Este Edital e seus anexos estarão à disposição dos interessados, no sítio www.emap.ma.gov.br, no link transparência/licitações, podendo ainda ser adquirido gratuitamente na CSL/EMAP, durante os dias úteis, das 08:00 às 12:00 horas e das 13:00 às 17:00 horas, através da apresentação de dispositivo de armazenagem eletrônica (cd, pen drive etc.).

16.13 Até a data e hora de início da sessão pública prevista neste Edital, a licitante deverá acessar o sítio da EMAP www.emap.ma.gov.br, no link Licitações para acompanhamento de quaisquer alterações, erratas, adiamento, esclarecimentos, julgamento de impugnação, revogação, anulação e demais informações complementares referentes ao presente Edital.

16.14 Caso seja necessária a interrupção da sessão, os autos do processo ficarão sob a guarda do Pregoeiro, que designará nova data para a continuação dos trabalhos.

16.15 São partes integrantes deste Edital os seguintes Anexos:

ANEXO I – Termo de Referência.
ANEXO II -- Modelo de Proposta.
ANEXO III – Modelo de Termo de Compromisso de Cumprimento da Legislação Trabalhista, Previdenciária e de Saúde e Medicina do Trabalho.
ANEXO IV – Declaração de Microempresa ou Empresa de Pequeno Porte
ANEXO V – Declaração das Condições de Empregabilidade de Menor.
ANEXO VI -- Questionário para realização de diligências apropriadas
ANEXO VII – Minuta do Contrato.
ANEXO VIII – Normas de Segurança, Saúde e Meio Ambiente do Porto do Itaqui.

São Luís/MA, 11 de junho de 2024.

Ciane Sozinho de Souza
Gerente de Compras e Contratos da EMAP

PREGÃO ELETRÔNICO N° 021/2024 – EMAP

ANEXO I

TERMO DE REFERÊNCIA

1. RESUMO DO OBJETO

Constitui objeto deste Termo de Referência, a aquisição de evolução tecnológica de Proteção de Borda, estações de trabalho e servidores da EMAP, bem como serviço de instalação e configuração, conforme condições, quantidades e exigências estabelecidas neste termo.

2. DETALHAMENTO DO OBJETO

2.1. DESCRIÇÃO DOS PRODUTOS:

MODELO DE ORÇAMENTO		
LOTE ÚNICO		
ITEM	DESCRIÇÃO	QUANTIDADE
1	Solução de Next Generation Firewall em Alta Disponibilidade	2
2	Solução de Gerenciamento Centralizado	1
3	Solução de detecção e resposta estendidas para estações de trabalho e servidores.	700
4	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 200 usuários - 36 meses	1
5	Serviço de instalação, configuração e migração da solução	1

2.2. ITEM 01: SOLUÇÃO DE SOLUÇÃO DE NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE - NGFW

2.3.1. Deve possuir throughput de, no mínimo, 8 (oito) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

2.3.2. Deve possuir throughput de, no mínimo, 4 (quatro) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

2.3.3. Deve suportar, no mínimo, 1.000.000 (um milhão) conexões simultâneas;

2.3.4. Deve suportar, no mínimo, 130.000 (cento e trinta mil) novas conexões por segundo;

2.3.5. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de /10/100/1000 Mbps do tipo RJ-45;

2.3.6. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1/10 Gbps do tipo SFP/SFP+;

2.3.7. Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps para gerenciamento;

2.3.8. Deve possuir, no mínimo, 1 (uma) interface física dedicada para o recurso de alta disponibilidade;

2.3.9. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

2.3.10. Deve possuir armazenamento interno de, no mínimo, 240 (duzentos e quarenta) GB para registro de logs;

2.3.11. Deve suportar fonte de alimentação elétrica interna redundante capaz de operar entre 120 à 240 VAC;

2.3.12. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responda. Caso o equipamento não possua essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento;

2.3.13. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

2.3.14. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

2.3.15. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

2.3.16. As funcionalidades de estabelecimento de túneis de VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

2.3.17. Todos os componentes da solução deverão operar em alta disponibilidade;

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

2.3.19. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

2.3.20. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.2.20.1. Agregação de links 802.3ad e LACP;

1.2.20.2. Policy based routing ou policy based forwarding;

1.2.20.3. Roteamento multicast (PIM-SM);

1.2.20.4. DHCP Relay;

1.2.20.5. DHCP Server;

1.2.20.6. Jumbo Frames;

1.2.20.7. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

1.2.20.8. Suportar sub-interfaces ethernet logicas;

2.3.21. Deve suportar os seguintes tipos de NAT:

1.2.21.1. Nat dinâmico (Many-to-1);

1.2.21.2. Nat dinâmico (Many-to-Many);

1.2.21.3. Nat estático (1-to-1);

1.2.21.4. NAT estático (Many-to-Many);

1.2.21.5. Nat estático bidirecional 1-to-1;

1.2.21.6. Tradução de porta (PAT);

1.2.21.7. NAT de Origem;

1.2.21.8. NAT de Destino;

1.2.21.9. Suportar NAT de Origem e NAT de Destino simultaneamente;

2.3.22. Deve implementar Network Prefix Translation (NPTv6);

2.3.23. Enviar log para sistemas de monitoração externos;

2.3.24. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

2.3.25. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

2.3.26. Proteção contra anti-spoofing;

2.3.27. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

2.3.28. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

2.3.29. Suportar a OSPF graceful restart;

2.3.30. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;

2.3.31. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);

2.3.32. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

2.3.33. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

2.3.34. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

2.3.35. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

2.3.36. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

1.2.36.1. Em modo transparente;

1.2.36.2. Em layer 3;

2.3.37. A configuração em alta disponibilidade deve sincronizar:

1.2.37.1. Sessões;

1.2.37.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

1.2.37.3. Certificados de-criptografados;

1.2.37.4. Associações de Segurança das VPNs;

1.2.37.5. Tabelas FIB;

1.2.37.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

2.3.38. CONTROLE POR POLÍTICA DE FIREWALL

1.2.38.1. Deverá suportar controles por zona de segurança;

1.2.38.2. Controles de políticas por porta e protocolo;

1.2.38.3. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

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

1.2.38.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

1.2.38.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

1.2.38.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

1.2.38.8. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);

1.2.38.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

1.2.38.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

1.2.38.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2 , TLS 1.2 e 1.3;

1.2.38.12. Controle de inspeção e de-criptografia de SSH por política;

1.2.38.13. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

1.2.38.14. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;

1.2.38.15. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

1.2.38.16. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

1.2.38.17. Suporte a objetos e regras IPV6;

1.2.38.18. Suporte a objetos e regras multicast;

1.2.38.19. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.2.38.20. Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.

2.3.39. CONTROLE DE APLICAÇÕES

1.2.39.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

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

1.2.39.1.2. Reconhecer pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.2.39.1.3. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;

1.2.39.1.4. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.2.39.1.5. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

1.2.39.1.6. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de

políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

1.2.39.1.7. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.2.39.1.8. Atualizar a base de assinaturas de aplicações automaticamente;

1.2.39.1.9. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

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

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

1.2.39.1.12. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

1.2.39.1.13. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

1.2.39.1.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações customizadas;

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

1.2.39.1.16. Deve alertar o usuário quando uma aplicação for bloqueada;

1.2.39.1.17. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.2.39.2. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:

1.2.39.2.1. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesma, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;

1.2.39.2.2. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;

1.2.39.2.3. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

2.3.40. PREVENÇÃO DE AMEAÇAS

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

1.2.40.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real;

1.2.40.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

1.2.40.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

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

1.2.40.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma

geral e assinatura a assinatura;

1.2.40.7. Deve permitir o bloqueio de vulnerabilidades.

1.2.40.8. Deve permitir o bloqueio de exploits conhecidos.

1.2.40.9. Deve incluir proteção contra ataques de negação de serviços.

1.2.40.10. Deverá possuir os seguintes mecanismos de inspeção de IPS:

1.2.40.11. Análise de padrões de estado de conexões;

1.2.40.12. Análise de decodificação de protocolo;

1.2.40.13. Análise para detecção de anomalias de protocolo;

1.2.40.14. Análise heurística;

1.2.40.15. IP Defragmentation;

1.2.40.16. Remontagem de pacotes de TCP;

1.2.40.17. Bloqueio de pacotes malformados.

1.2.40.18. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

1.2.40.19. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

1.2.40.20. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

1.2.40.21. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

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

1.2.40.23. Possuir assinaturas para bloqueio de ataques de buffer overflow;

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

1.2.40.25. Identificar e bloquear comunicação com botnets;

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

1.2.40.27. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.2.40.28. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

1.2.40.29. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação;

1.2.40.30. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

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

1.2.40.32. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião

(spyware) e worms;

1.2.40.33. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos;

1.2.40.34. Rastreamento de vírus em pdf;

1.2.40.35. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);

1.2.40.36. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

1.2.40.37. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

1.2.40.38. Domínio suspeito identificado;

1.2.40.39. ID de assinatura de detecção;

1.2.40.40. Usuário logado na estação/servidor que originou o tráfego;

1.2.40.41. Aplicação;

1.2.40.42. Porta de destino;

1.2.40.43. IP de origem;

1.2.40.44. IP de destino;

1.2.40.45. Horário;

1.2.40.46. Ação do firewall;

1.2.40.47. Severidade;

1.2.40.48. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

1.2.40.49. A análise automática deve incluir, no mínimo, as seguintes características:

1.2.40.50. Padrões de consulta;

1.2.40.51. Entropia;

1.2.40.52. Análise de frequência n-gram de domínios;

1.2.40.53. Taxa de consultas.

1.2.40.54. Deve possuir a capacidade de analisar em tempo real a requisições de DNS e acesso a novas assinaturas de DNS;

2.3.41. ANÁLISE DE MALWARES MODERNOS

1.2.41.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

1.2.41.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;

1.2.41.3. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, Mac OS X, Android, Linux.

1.2.41.4. A solução deve possuir a capacidade de extrair e analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

1.2.41.5. A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

1.2.41.6. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

1.2.41.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

1.2.41.8. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

1.2.41.9. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

1.2.41.10. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

1.2.41.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

1.2.41.12. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

1.2.41.13. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;

1.2.41.14. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

1.2.41.15. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

1.2.41.16. A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executem esta função.

1.2.41.17. Deve prevenir contra ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.

1.2.41.18. Deve ser capaz de aplicar de forma complementar às assinaturas de antivirus a inspeção inline através de Machine learning em tempo real arquivos tipo PE (portable executable), ELF (executable and linked format) e Arquivos Microsoft Office, bem como, scripts PowerShell e shell script em tempo real para malwares desconhecidos;

1.2.41.19. FILTRO DE URL

1.2.41.20. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

1.2.41.21. Deve suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

1.2.41.22. Deve possuir pelo menos 60 categorias de URLs;

1.2.41.23. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

1.2.41.24. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;

1.2.41.25. Deve suportar a capacidade de criação de políticas baseadas no controle por URL ou

categoria de URL;

1.2.41.26. Deve suportar a criação categorias de URLs customizadas;

1.2.41.27. Deve possuir a função de exclusão de URLs do bloqueio;

1.2.41.28. Deve permitir a customização de página de bloqueio;

1.2.41.29. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

1.2.41.30. Deve permitir controlar o envio de credenciais corporativas somente para categorias de URLs permitidas;

1.2.41.31. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

1.2.41.32. Deve prover análise em tempo real do conteúdo web e dessa forma permitir o bloqueio de páginas maliciosas antes mesmo da atualização das bases de dados de URLs do fabricante da solução;

1.2.41.33. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

2.3.42. VPN

1.2.42.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.2.42.2. Suportar IPSec VPN e SSL Vpn;

1.2.42.3. A VPN IPSEc deve suportar:

1.2.42.4. 3DES;

1.2.42.5. Autenticação MD5 e SHA-1;

1.2.42.6. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

1.2.42.7. Algoritmo Internet Key Exchange (IKEv1 e v2);

1.2.42.8. AES 128 e 256 (Advanced Encryption Standard);

1.2.42.9. Autenticação via certificado IKE PKI.

1.2.42.10. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

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

1.2.42.12. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

1.2.42.13. Suportar a instalação dos clientes de VPN em sistemas operacionais Windows e MacOS;

1.2.42.14. Suportar e estar licenciado para acesso remoto Client-to-Site para no mínimo 50 (cinquenta) conexões simultâneas;

1.2.42.15. A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;

1.2.42.16. A solução deve permitir bloquear o acesso dos usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados.

2.3.43. SD-WAN

1.2.43.1. Deve ser capaz de agregar vários links em uma interface virtual;

1.2.43.2. Deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jiter e Packet Loss, onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras da interface virtual;

1.2.43.3. Deve poder adicionar e equilibrar, no mínimo, 06 interfaces de dados (links e VPNS);

1.2.43.4. Deve suportar a agregação de túneis de VPN IPSec e balancear o tráfego entre eles e inserir essa interface agregada à Interface Virtual;

1.2.43.5. Deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface virtual;

1.2.43.6. Deve possibilitar a distribuição de trafego entre os links que compõe a interface virtual, a critério do administrador;

1.2.43.7. Deve suportar a critério do administrador uma topologia Full-mesh;

1.2.43.8. Deve permitir configurar acesso direto à Internet para aplicações tipo SaaS;

1.2.43.9. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponiveis que está orientado ao mesmo destino.

1.2.43.10. O dispositivo de SD-WAN deve utilizar Forward Error Correction (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro

caminho.

1.2.43.11. Garantia mínima de 36 (trinta e seis) meses incluindo todas as licenças necessárias para as funcionalidades

2.3. ITEM 02: SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

2.3.1. Deve suportar estar hospedada na nuvem do fabricante em datacenter com no mínimo certificação SOC2, ou em appliance virtual e deve ser compatível/homologado para no mínimo VMware ESXi versão 7.0;

2.3.2. Deve possuir capacidade de Armazenamento de até 7TB;

2.3.3. A gerência centralizada deve possuir modulo de solução para validação de conformidade de acordo com normas de mercado conforme exemplo.

2.3.4. ISO 27001 e ISO 27002;

2.3.5. PCI-DSS;

2.3.6. NIST 800-41

2.3.7. GDPR (base da norma LGPD);

2.3.8. A solução para validação de conformidade, deve ser contemplada para o primeiro ano de projeto para adequação as novas normas de mercado que a instituição irá seguir. Não será permitido licenciamento mensalidade “trial”, ou seja, deve ser considerado uma licença de uso anual, podendo ela ser renovada por um período maior.

2.3.9. Caso a solução não possua tal modulo, será permitido composição com soluções de mercado, nao sendo elas soluções abertas “Software Livre”.

2.3.10. Deve ser capaz de controlar todos os equipamentos da plataforma de segurança em uma única

console;

2.3.11. Deve permitir a criação de dashboard customizados para exibir informações de no mínimo:

2.3.12. Prevenção de Ameaças;

2.3.13. Uso de aplicações;

2.3.14. Segurança de DNS;

2.3.15. Uso de Rede;

2.3.16. Informações de Sandbox.

2.3.17. Deve possuir dashboard capaz de apresentar a saúde dos dispositivos gerenciados através de escores, estatisticas e tendências;

2.3.18. Deve possuir dashboard capaz de apresentar informações de rede sumarizadas bem como por tráfego, usuários e endereços IPs;

2.3.19. Deve prover visão de 360 graus relativa a atividades de ameaças bem como suas tendências;

2.3.20. Deve em relação a ameaças apresentar dashboards de ameaças para:

2.3.21. Aplicações mais impactadas;

2.3.22. Usuários mais impactados;

2.3.23. Políticas de segurança mais impactadas.

2.3.24. Deve apresentar sumario executivo contendo:

2.3.25. aplicações de maiores riscos;

2.3.26. atividades web maliciosas;

2.3.27. Atividades de Sandbox;

2.3.28. Deve permitir gerar relatórios de boas práticas;

2.3.29. Deve apresentar resumo da adoção de serviços de segurança pelos equipamentos gerenciados;

2.3.30. Deve ser capaz de criar políticas de segurança contendo:

2.3.31. Regras de Antivirus e antispyware;

2.3.32. Segurança de DNS;

2.3.33. Filtro de URLs;

2.3.34. Proteção de vulnerabilidades;

2.3.35. Regras de descriptografia;

2.3.36. Regras de Rede e QoS;

2.3.37. Regras de NAT.

2.3.38. Deve ser capaz de configurar autenticação;

2.3.39. Deve permitir a criação de listas externas a serem utilizadas pelas políticas de segurança;

2.3.40. Deve permitir a criação de agendamentos;

2.3.41. Deve trazer informações relativas a postura de segurança e recomendações de upgrade de software;

2.3.42. Deve analisar a necessidade de criação de novas regras de segurança;

2.3.43. Deve trazer informações relativas a capacidade dos dispositivos gerenciados contendo:

2.3.44. Métricas de utilização;

2.3.45. Mapa de calor do uso de recursos.

2.3.46. O analisador de capacidade deve ser capaz de emitir alertas contendo no mínimo:

2.3.47. Recursos de criptografia;

2.3.48. Anomalias;

2.3.49. Capacidade da Tabela ARP;

2.3.50. Capacidade de Objetos e grupos;

2.3.51. Capacidade máxima de CPU;

2.3.52. Capacidade máxima de Memória;

2.3.53. Capacidade máxima de tabelas de sessões;

2.3.54. Capacidade máxima de configurações;

2.3.55. HA Status;

2.3.56. Aumento de latência.

2.3.57. Dashboard contendo informações relativas ao SDWAN contendo:

2.3.58. Saúde das aplicações;

2.3.59. Aplicações mais impactadas;

2.3.60. Saúde dos links;

2.3.61. Lista de piores links.

2.3.62. Deve apresentar lista dos dispositivos impactados pelos CVEs;

2.3.63. Análise de causas prováveis relativas a alta processamento;

2.3.64. Garantia mínima de 36 (trinta e seis) meses incluindo todas as licenças necessárias para as funcionalidades

2.4. ITEM 03: SOLUÇÃO DE DETECÇÃO E RESPOSTA ESTENDIDAS PARA ESTAÇÕES DE TRABALHO E SERVIDORES

2.4.1. A entidade requer uma solução de Extended Detection & Response, tecnologia que amplia as capacidades de detecção e resposta além de soluções de endpoints tradicionais (EDR, Antivírus e EPP);

2.4.2. A tecnologia deve incluir ações de resposta a incidentes em endpoints e permitir integração com soluções SOAR (Security Orchestration Automation & Response);

2.4.3. A solução deve ser reconhecida como líder no último relatório Forrester Wave 2021: Endpoint Security as a Service;

2.4.4. A solução deve ter participado das rodadas de detecção MITRE ATT&CK TTP (APT3, APT29) e deve ter participado do teste de detecção e proteção dos anos de 2021/2022 (Carbanak & FIN7/Wizard Spyder & Sandworm respectivamente).

2.4.5. A ferramenta de endpoint XDR, deve possuir a capacidade de apresentar informações de telemetria do dispositivo (computadores e servidores) que tem o agente instalado, mesmo que esse endpoint não apresente alertas ou incidentes de segurança.

2.4.6. A solução deve ter a capacidade de detecção e prevenção contra ataques cibernéticos mesmo que o agente instalado no dispositivo (computadores e servidores) não tenham conexão com o console de gerenciamento centralizado e com a Internet;

2.4.7. Prevenção contra Técnicas de Exploração de Vulnerabilidade

2.4.8. A solução de Endpoint XDR, deve possuir na sua console de gerenciamento centralizado a matriz do MITRE ATT&CK como padrão na apresentação de técnicas de exploração.

2.4.9. Detecção e prevenção do mecanismo de identificação das propriedades de um sistema por um Exploit Kit (técnica conhecida como Exploit Kit Fingerprint) sem a necessidade de usar assinaturas, padrões ou heurísticas;

2.4.10. Detecção de técnicas de exploração sem a necessidade de uso de assinaturas, padrões ou heurísticas, principalmente focadas na prevenção de exploits lógicos, processos vulneráveis e exploits de sistema operacional, para sistemas Microsoft Windows;

2.4.11. Mitigação de vulnerabilidades conhecidas, desconhecidas e de dia zero;

2.4.12. Suporte a identificação de diferentes técnicas de exploração de vulnerabilidades, entre as quais Return Oriented Programming (ROP), Heap Spray, Jit Spray, Shpell link, Structured Exception Handler (SEH), etc);

2.4.13. Proteção de aplicativos contra técnicas de exploração por padrão e de forma nativa;

2.4.14. Entre os aplicativos protegidos por padrão devem estar: Firefox, Internet Explorer, Microsoft Word, Microsoft Excel, várias versões do Flash Player, Microsoft Silverlight, Apache, IIS entre outros;

2.4.15. Capacidade de usar módulos de proteção contra técnicas de exploração em qualquer aplicação ou processo, incluindo aqueles desenvolvidos internamente;

2.4.16. Capacidade de criar automaticamente um snapshot da memória RAM ao impedir a execução de uma técnica de exploração, a fim de fornecer dados forenses sobre o evento;

2.4.17. Capacidade de realizar análise avançada do status da memória quando um alerta de prevenção de exploração é gerado;

2.4.18. Permitir a configuração de perfis de proteção em modo de prevenção ou monitoramento;

2.4.19. Capacidade de encerramento do processo em que foi identificada a tentativa de execução de uma técnica de exploração, desde que não seja um processo crítico do sistema operacional;

2.4.20. Prevenção de técnicas de exploração usando Dylib-Hijacking para Mac OS;

2.4.21. Prevenção de técnicas de exploração usando Return Oriented Program (ROP) para Mac OS.

2.4.22. Prevenção de técnicas de exploração usando JIT para Mac OS.

2.4.23. Prevenção de técnicas de exploração que buscam seqüestrar o fluxo de controle de um processo monitorando tentativas de enumeração de alocação de memória para sistemas operacionais Linux.

2.4.24. Prevenção de técnicas de exploração que buscam redirecionar fluxos de entrada e saída padrão para soquetes de rede para sistemas operacionais Linux;

2.4.25. Prevenção de técnicas de exploração que usam Return Oriented Program (ROP) para sistemas operacionais Linux.

2.4.26. Prevenção do uso de certas áreas de memória que são comumente utilizadas para armazenar payload de um ataque baseado em técnicas de heap spray, para sistemas operacionais Linux.

2.4.27. Proteção contra ataques de webshells de PHP em servidores Linux.

2.4.28. Capacidade de fornecer proteção contra ataques que utilizam técnicas de exploração de vulnerabilidades sem exigir que a máquina protegida possua uma conexão com o console de gerenciamento.

2.4.29. Identificação de ataques de pós-exploração.

2.4.30. A solução de Endpoint XDR, deve possuir na sua console de gerenciamento centralizado a matriz do MITRE ATT&CK como padrão para detalhar as ações técnicas utilizadas na exploração.

2.4.31. Identificação e prevenção de tentativas de escalar privilégios no nível do Kernel. Essa proteção deve poder ser usada em agentes instalados em endpoints com Sistemas Operacionais Windows, Mac e Linux;

2.4.32. Detecção e encerramento de comportamentos considerados maliciosos através da análise contínua da cadeia de eventos que ocorrem em um endpoint. Essa detecção deve considerar vários eventos e não apenas um evento para fornecer um veredicto de atividade maliciosa. A detecção deve utilizar várias regras pré-configuradas, que devem ter a capacidade de analisar vários eventos e não apenas um evento;

2.4.33. A proteção não deve exigir uma conexão da máquina protegida com a console de

gerenciamento;

2.4.34. Prevenção contra malware conhecido.

2.4.35. Deve fornecer proteção na memória contra o uso do Mimikatz ou ferramenta de extração de senha semelhante.

2.4.36. Geração de hashes de processos em execução e verificação de veredictos em uma nuvem de inteligência de ameaças;

2.4.37. Envio automático de executáveis, quando seu hash é desconhecido, para análise em um sandbox localizado na nuvem, a fim de determinar se são maliciosos ou benignos. Essa proteção deve estar disponível para os sistemas operacionais Windows, Mac, Linux e Android;

2.4.38. Capacidade de prevenir contra ataques de shell reversos (Reverse Shell) para sistemas operacionais Linux.

2.4.39. Capacidade de escanear o computador comparando os hashes dos arquivos executáveis que estão armazenados no computador com base de veredicto em uma nuvem de inteligência de ameaças;

2.4.40. Capacidade de enviar arquivos classificados como maliciosos para quarentena, sejam eles identificados no momento da tentativa de execução ou no momento da identificação por meio de uma varredura;

2.4.41. Deve ter um módulo de prevenção de ransomware, que deve impedir um processo de criptografia identificando tentativas de modificação de arquivos;

2.4.42. Capacidade de proteção contra ataques de mineração de bitcoin para dispositivos Linux, detectando-os por seu comportamento e não somente assinatura de hash.

2.4.43. Prevenção contra malware desconhecido.

2.4.44. Deve usar um modelo matemático gerado a partir de aprendizado de máquina para comparar um grande número de características de um arquivo executável, de forma estática, para determinar se ele é malicioso. Essa proteção deve estar disponível para os sistemas operacionais Windows, Linux e Mac;

2.4.45. Deve permitir a criação de listas de bloqueio de arquivos a partir de seu hash para que o administrador possa determinar quais aplicativos podem ser executados no ambiente;

2.4.46. Capacidade de identificar se a macro contida em um documento do Word ou Excel é maliciosa, sem precisar executar a macro ou observar seu comportamento ou execução, para

determinar se é maliciosa;

2.4.47. Capacidade de proteção contra malware sem a necessidade de assinaturas, padrões e/ou heurísticas;

2.4.48. Deve ser possível configurar as políticas em modo de prevenção ou monitoramento;

2.4.49. Deve permitir que os arquivos detectados como maliciosos sejam colocados em quarentena, automaticamente ou sob demanda;

2.4.50. Envio de arquivos desconhecidos de forma automática para um sandbox para serem analisados adicionalmente a todos os recursos de detecção/bloqueio local no agente em execução no Windows, Linux e MacOS e permitir visualizar os relatórios de análise detalhados e baixá-los a qualquer momento no console.

2.4.51. Envio de executáveis, quando seu hash é desconhecido, para análise em um sandbox localizado na nuvem, a fim de determinar se são maliciosos ou benignos. Essa proteção deve estar disponível para os sistemas operacionais Windows, Mac, Linux e Android;

2.4.52. Scan periódico/sob demanda de arquivos executáveis.

2.4.53. Permite a verificação de arquivos executáveis sem a necessidade de assinaturas;

2.4.54. Permite agendar a verificação de arquivos semanal ou mensalmente;

2.4.55. Permite definir o dia e a hora em que a verificação será iniciada;

2.4.56. O consumo de recursos no momento da verificação não deve afetar a experiência do usuário;

2.4.57. Permite habilitar a verificação de dispositivos de armazenamento removíveis;

2.4.58. Permite criar listas de exceção (Allow List) de pastas para que sejam excluídas do processo de verificação;

2.4.59. Permite que arquivos identificados como maliciosos sejam colocados em quarentena, se a política estiver configurada dessa forma;

2.4.60. Deve permitir que o usuário, a qualquer momento, inicie o scan de um arquivo presente no disco rígido de forma manual;

2.4.61. O scan de arquivos deve ser capaz de realizar análise estática em arquivos desconhecidos para determinar se eles são maliciosos, bem como enviar esses arquivos desconhecidos para o serviço de análise em nuvem para análise.

2.4.62. Restrições de execução e exceções de política.

2.4.63. Deve permitir a criação de restrições na execução de arquivos de uma determinada pasta;

2.4.64. Deve permitir a criação de restrições na execução de arquivos de recursos compartilhados;

2.4.65. Deve permitir a criação de restrições na execução de arquivos de dispositivos USB ou CD/DVD.

2.4.66. Deve aplicar as restrições configuradas sem a necessidade de uma conexão com o console de gerenciamento;

2.4.67. Deve possuir políticas de restrição de criação de processo filho configuradas por padrão;

2.4.68. Deve permitir a criação de exceções para permitir a execução de arquivos de determinadas pastas;

2.4.69. Deve permitir a criação de exceções para permitir a execução de processos filho;

2.4.70. Deve permitir a criação de exceções para permitir a execução de arquivos de pastas em dispositivos de armazenamento removíveis;

2.4.71. Deve permitir a criação de políticas de restrição em modo de bloqueio ou apenas monitoração.

2.4.72. Restrição do uso de mídias removíveis.

2.4.73. A solução deve ter a capacidade de permitir e bloquear o uso de discos removíveis para os tipos de dispositivos (computadores e servidores) nos sistemas operacionais Windows e MAC;

2.4.74. A solução deve ter a capacidade de permitir e bloquear o uso de discos removíveis através de políticas de segurança customizadas na gerência centralizada da solução de XDR para encerramento dos processos do sistema operacional Linux;

2.4.75. Deve permitir a geração de perfis que gerenciam as seguintes características de bloqueio de porta USB quando os seguintes tipos de dispositivos estiverem conectados: discos rígidos, unidades de CD-ROM externas conectadas por USB, dispositivos de armazenamento removíveis portáteis conectados por USB, disquetes externos com conexão USB , adaptadores de rede em formato USB;

2.4.76. Deve permitir a geração de perfis de exceção para poder conectar dispositivos a portas

USB utilizando os seguintes parâmetros: tipo de dispositivo (discos rígidos, unidades externas de CD-ROM com conexão USB, dispositivos de armazenamento removíveis portáteis com conexão USB, unidades de disco, disquetes externos com conexão USB), tipo de permissão para atribuir (leitura/gravação ou somente leitura), fabricante (deve conter uma lista padrão), produto (deve conter uma lista padrão) e número de série. O tipo de dispositivo, tipo de licença e parâmetros do fabricante devem ser obrigatórios.

2.4.77. Deve permitir a criação de políticas que utilizem os perfis de bloqueio e exceção por grupo de máquinas ou de forma global;

2.4.78. As políticas geradas devem poder ser atribuídas a um determinado computador ou a um grupo de computadores previamente definido;

2.4.79. Você deve permitir a criação de exceções permanentes usando os seguintes parâmetros: tipo de dispositivo (disco rígido, unidades de CD-ROM externas conectadas por USB, dispositivos de armazenamento removíveis portáteis conectados por USB, unidades de disquete externas conectadas por USB), tipo de permissão para atribuir (leitura/gravação ou somente leitura), fabricante (deve conter uma lista padrão), produto (deve conter uma lista padrão) e número de série. O tipo de dispositivo, tipo de licença e parâmetros do fabricante devem ser obrigatórios. Essas exceções permanentes não devem depender de serem aplicadas a uma política para entrar em vigor;

2.4.80. Deve permitir a criação de regras de exceção temporárias a partir de uma violação de política de uso de mídias removíveis detectada na console de administração;

2.4.81. Deve mostrar as violações de política que foram registradas, mostrando o seguinte: hora, computador, usuário, endereço IP, tipo de dispositivo, produto, fabricante e número de série do dispositivo que tentou se conectar;

2.4.82. Essa funcionalidade deve ser compatível com os sistemas operacionais Windows e Mac.

2.4.83. Firewall de host

2.4.84. Essa funcionalidade deve ser compatível com os sistemas operacionais Windows e Mac;

2.4.85. Os seguintes recursos devem estar disponíveis para sistemas operacionais Windows:

2.4.86. Controle todas as comunicações de entrada e saída usando endereços IP.

2.4.87. Permitir que as regras sejam aplicadas de acordo com a localização do dispositivo, por exemplo, que só se apliquem se estiverem na rede interna.

2.4.88. O produto deve ser capaz de determinar, por meio da configuração, se o dispositivo está dentro ou fora da organização.

2.4.89. A regra poderá especificar endereços locais ou remotos, bem como portas locais ou remotas. O protocolo também pode ser especificado dentro destas quatro opções: ICMP, TCP, UDP, ICMPv6.

2.4.90. As seguintes funcionalidades devem estar disponíveis para sistemas operacionais Mac:

2.4.91. Permitir habilitar ou desabilitar o firewall nativo do sistema operacional.

2.4.92. Permitir ou bloquear comunicações de rede de entrada.

2.4.93. Ativar o modo furtivo

2.4.94. Crie exclusões por aplicativo para permitir ou bloquear especificamente programas usando a funcionalidade do sistema operacional conhecida como BlundleID

2.4.95. Dados de Telemetria de Endpoint

2.4.96. O produto deve ser capaz de capturar, no mínimo, as seguintes ações no nível de terminal em sistemas operacionais Windows:

2.4.97. Processo executado, incluindo hora de início, tamanho do arquivo associado.

2.4.98. Atividades de criação, escrita, renomeação, exclusão, modificação e criação de links simbólicos de um arquivo;

2.4.99. Os seguintes parâmetros devem ser registrados quando os arquivos DLL são carregados: caminho completo, endereço base, id do processo ou thread que o está carregando, tamanho da imagem, assinatura, valores de hash calculados com os algoritmos MD5 e SHA256 da DLL arquivo, tamanho do arquivo, tempo de acesso ao arquivo;

2.4.100. Criação e encerramento de processos;

2.4.101. Injeções em threads de processo. ID do encadeamento pai, ID do encadeamento novo ou encerrado, processo que iniciou o encadeamento (se for um processo diferente);

2.4.102. Protocolos de rede: solicitações DNS e respostas UDP, conexão HTTP, desconexão HTTP, análise de proxy HTTP;

2.4.103. Estatísticas da rede. Volume no momento do envio por um link TCP. Volume recebido por meio de um link TCP;

2.4.104. Definição ou exclusão de valores do registro. Criar, modificar, excluir, adicionar, restaurar e salvar chaves de registro;

2.4.105. Sessões do sistema operacional. login, logoff, conexão e desconexão. Considerando os seguintes atributos: login interativo, id da sessão, estado da sessão e se a sessão é local ou remota;

2.4.106. Status do computador: inicialização, suspensão, reinicialização. Com os seguintes atributos: nome do computador, versão do sistema operacional, domínio, status anterior e atual;

2.4.107. logs de eventos do windows.

2.4.108. O produto deve ser capaz de capturar, no mínimo, as seguintes ações no nível de endpoint em sistemas operacionais Mac:

2.4.109. Crie, escreva, exclua, renomeie, altere o caminho e abra arquivos. Com os seguintes atributos: caminho completo do arquivo modificado antes e depois de sua modificação. Geração de hashes com algoritmos SHA256 e MD5 para o arquivo após sua modificação;

2.4.110. Iniciando e parando processos, com os seguintes parâmetros: ID do processo para o processo pai, ID do processo, caminho completo, argumentos de linha de comando, nível de integridade para determinar se o processo está sendo executado com privilégios elevados, valores de hash calculados com algoritmos MD5 e SHA256, detalhes da assinatura ou do certificado usado para assinar o arquivo;

2.4.111. O produto deve ser capaz de capturar, no mínimo, as seguintes ações no nível de terminal em sistemas operacionais Linux:

2.4.112. Para arquivos, ações de criação, abertura, gravação e exclusão, incluindo o caminho completo do arquivo e o hash do arquivo (para determinados arquivos e somente se o arquivo foi gravado). Copie ou renomeie os arquivos, incluindo os caminhos completos dos arquivos originais e modificados. Ações para alterar o proprietário (chown) e o modo (chmod) dos arquivos, incluindo o caminho completo do arquivo, bem como o novo proprietário ou novos atributos;

2.4.113. Processos. Criação de processos, com os seguintes atributos: ID do processo filho, id do processo pai, caminho completo da imagem do processo, linha de comando do processo, valores de hash calculados com os algoritmos SHA256 e MD5. Encerramento de processos, incluindo o ID do processo.

2.4.114. Capacidade de detecção baseada em dados de identidade (IAM)

2.4.115. A solução deve ter a capacidade de ingerir dados de identidade de fontes como Azure

AD, Okta ou PingOne;

2.4.116. Deve identificar quando um usuário desativado tenta autenticar;

2.4.117. Deve identificar quando um usuário procura autenticar a partir de um novo ASN;

2.4.118. Deve alertar quando um usuário procura se autenticar a partir de um país incomum pela primeira vez;

2.4.119. Deve alertar quando um usuário procura se autenticar em um país diferente;

2.4.120. Deve alertar uma anomalia quando um usuário procura se autenticar em vários países em um curto período de tempo, o que seria impossível;

2.4.121. Deve alertar quando uma conta de dispositivo e não uma conta de usuário tenta autenticar;

2.4.122. Deve alertar quando uma conta de serviço e não uma conta de usuário tenta autenticar;

2.4.123. Deve alertar quando um usuário tenta se autenticar de forma suspeita após não ter feito isso em um período de tempo;

2.4.124. Deve alertar quando um usuário tentar se autenticar com um sistema operacional novo ou anormal.

2.4.125. Análise de alertas e investigação

2.4.126. Deve ter uma console em nuvem que permita visualizar alertas gerados de diferentes fontes;

2.4.127. Deve ser capaz de exibir o número total de alertas e incidentes e deve incluir a capacidade de filtrar informações de forma flexível;

2.4.128. Deve permitir a criação de uma sequência gráfica que correlaciona alertas individuais para descrever a sequência de um ataque; (Pro per EP)

2.4.129. Deve apresentar informações específicas sobre cada processo envolvido na sequência do ataque; (Pro per EP)

2.4.130. Deve apresentar os dados relacionados ao perfil de comportamento e a execução de cada processo envolvido na cadeia do ataque; (Pro per EP)

2.4.131. Deve exibir um aviso quando um determinado executável, que faz parte da sequência gráfica, se comporta de forma suspeita. (Pro per EP)

2.4.132. Deve apresentar dados gerais da execução de um processo que faz parte da sequência gráfica, entre os quais estão caminho de execução, nome do usuário que executou o processo,

tempo de execução, entidade que assinou o processo, valor MD5 do executável relacionado ao processo, veredicto de análise de sandbox, valor SHA256 e linha de comando de execução. (Pro per EP)

2.4.133. Deve mostrar a atividade de cada processo identificado, em colunas por categorias. As categorias a serem incluídas devem incluir atividade de rede, atividade de arquivo, atividade de registro, módulos executados e tentativas de injeção de processo. (Pro per EP)

2.4.134. Deve usar aprendizado de máquina supervisionado e não supervisionado para estabelecer linhas de base do comportamento típico do usuário e do dispositivo e detectar desvios comportamentais que caracterizam atividade anômala. (Pro per EP)

2.4.135. Deve fornecer a capacidade de descodificar cadeias de caracteres codificados em base 64, utilizadas em comandos de execução para exibição em texto simples;

2.4.136. Deve ser capaz de identificar, de todas as atividades mencionadas acima, aquelas que são maliciosas ou altamente suspeitas e separá-las em uma categoria de fácil acesso ao analista.

2.4.137. Deve possuir Inteligência de ameaças compartilhada para distribuir inteligência de ameaças de crowdsourcing do serviço de análise de malware baseado em nuvem para firewalls, agentes de endpoint e serviços de detecção e resposta Para cada uma das atividades mencionadas acima, o produto deve exibir em colunas os seguintes dados: data, nome do computador, IP do host que gerou o alerta, nome de usuário, sistema operacional do host, tipo de atividade identificada, descrição da atividade identificada, nome do arquivo, nome do arquivo anterior, caminho do arquivo, caminho do arquivo anterior, valor MD5 do arquivo, valor SHA256 do arquivo, caminho do arquivo que foi o executor do arquivo, comando que foi utilizado pelo executor do arquivo, identificador do processo que foi o executor do arquivo, valor MD5 do executor do arquivo que foi a causa raiz do alerta, valor SHA256 do executor do arquivo que foi a causa raiz do alerta, indicador se o executor do alerta está assinado, entidade que assinou o arquivo que foi a causa raiz do alerta, caminho do arquivo que foi a causa raiz do alerta, comando do arquivo que foi a causa raiz do alerta, valor SHA 256 do arquivo que foi a causa raiz do alerta, indicador se o arquivo que foi a causa raiz do alerta está assinado, entidade que assina o arquivo que foi a causa raiz do alerta. (Pro per EP)

2.4.138. Deve mostrar se houve injeção de código ou se o protocolo RPC é utilizado em outro

processo a partir de um computador local ou remoto. (Pro per EP)

2.4.139. Deve fornecer graficamente a interação ocorrida com os endereços IP a serem investigados. (Pro per EP)

2.4.140. Deve ser capaz de mostrar diferentes opções de visualização, como localização geográfica ou os arquivos executáveis que geraram essa comunicação. (Pro per EP)

2.4.141. Deve fornecer graficamente a interação que existe entre um ou vários processos investigados. O gráfico deve mostrar a interação entre os processos, e se existe relação entre os computadores que executam tais processos, entre outros aspectos. (Pro per EP)

2.4.142. A solução deve possuir terminal remoto para acessar qualquer dispositivo (computadores windows, linux e MAC) para qualquer análise de processo, pastas e arquivos.

2.4.143. Gestão de Alertas e Incidentes

2.4.144. Deve possuir mecanismos de geração de alertas considerando o comportamento apresentado pelos processos computacionais.

2.4.145. Os alertas gerados pelo comportamento dos processos não devem utilizar assinaturas ou heurísticas.

2.4.146. Cada alerta gerado pelo comportamento dos processos deve ter uma descrição do comportamento identificado.

2.4.147. Cada alerta gerado deve ter uma classificação de acordo com sua severidade.

2.4.148. Deve permitir que o analista criem regras de comportamento para geração de alertas;

2.4.149. Deve permitir a geração de exceções ao comportamento dos processos que foram identificados como maliciosos ou suspeitos.

2.4.150. Deve permitir desabilitar, modificar ou eliminar os comportamentos que geram os alertas devido ao comportamento dos processos.

2.4.151. Deve permitir a importação de regras de comportamento suspeito;

2.4.152. Deve suportar o uso de indicadores tradicionais de comprometimento, incluindo caminhos de arquivos, nomes de arquivos, domínios, endereços IP e hashes.

2.4.153. Deve permitir desabilitar, modificar, exportar ou deletar um indicador de comprometimento através de um menu de contexto. (Pro per EP ou TB)

2.4.154. Deve permitir o gerenciamento dos indicadores de comprometimento por comportamento de processo e indicadores tradicionais de comprometimento por meio da console

de gerenciamento.

2.4.155. A solução deve ter a capacidade de criação de regras de automações que irão executar comandos no dispositivo com o agente XDR instalado assim que identificado um alerta de segurança.

2.4.156. Deve permitir que você isole um computador do próprio console de administração para que haja apenas comunicação entre o agente e o console. Deve oferecer a capacidade de adicionar comentários que expliquem por que um computador foi isolado.

2.4.157. Através da console centralizada da solução XDR, deve permitir a criação de regras customizadas pelo cliente para restringir a execução de softwares ou processos não autorizados nos computadores/servidores;

2.4.158. Deve definir outros processos e destinos (endereços IP) aos quais o computador pode se conectar, além do console em caso de isolamento.

2.4.159. Deve colocar em quarentena, sob demanda, arquivos maliciosos que foram detectados ou alertados, mas não bloqueados por políticas de prevenção definidas.

2.4.160. Deve exibir os detalhes dos arquivos que foram colocados em quarentena.

2.4.161. Deve permitir a exportação de todos os detalhes dos arquivos que foram colocados em quarentena em um arquivo com formato “tab-separated value” (TSV).

2.4.162. Deve permitir a restauração de um ou mais arquivos que foram colocados em quarentena simultaneamente.

2.4.163. O produto deve permitir uma conexão reversa com o dispositivo afetado, em versões superiores ao Windows 7 SP1, por meio de uma conexão remota para permitir as seguintes ações:

2.4.164. Encerrar o processo de execução

2.4.165. Suspender ou retomar o processo de execução

2.4.166. Adicionar um processo a um indicador de compromisso (IOC)

2.4.167. Cópia de binário em execução para investigação adicional

2.4.168. Deve permitir uma conexão reversa com o dispositivo afetado por meio de uma conexão remota para permitir a execução de scripts ou comandos no Python versão 3, no mínimo.

2.4.169. Deve permitir uma conexão reversa com o dispositivo afetado por meio de uma conexão remota para permitir a execução de scripts ou comandos no Powershell.

2.4.170. Deve permitir que unidades de armazenamento sejam acessadas remotamente, incluindo não apenas discos rígidos, mas também dispositivos de armazenamento removíveis. Deve permitir mover, renomear, excluir, baixar e fazer o hash de qualquer arquivo.

2.4.171. Deve permitir a criação de listas se permissão e bloqueio de execução de arquivos

2.4.172. Deve adicionar as informações de incidentes associadas quando um arquivo estiver na lista de permissões ou na lista de bloqueio.

2.4.173. Deve apresentar recomendações de ações corretivas a serem adotadas no endpoint baseado nos dados obtidos em alertas relacionados a ações suspeitas, permitindo a recuperação do ambiente a um estado prévio ao comprometimento. (Pro per EP + Host insights)

2.4.174. Deve realizar automaticamente a restauração ou deleção de arquivos, pastas e chaves de registro selecionadas pelo analista na tela de recomendações de correção. (Pro per EP)

2.4.175. Gestão de políticas e eventos

2.4.176. Gerenciamento centralizado de políticas, por meio de um console de gerenciamento em núvem.

2.4.177. Deve identificar claramente os eventos que foram relatados e/ou bloqueados e os que foram detectados.

2.4.178. Deve classificar o status dos incidentes em quatro níveis diferentes de severidade: alto, médio, baixo e informativo.

2.4.179. Deve classificar o status dos alertas em quatro níveis diferentes de severidade: alto, médio, baixo e informativo.

2.4.180. Deve-se agrupar alertas relacionados em incidentes, bem como fornecer um contexto dos mesmos.

2.4.181. Deve extrair os elementos importantes ou relevantes dos alertas e exibi-los como um resumo na tela de análise de incidentes.

2.4.182. Deve fornecer informações detalhadas, sob demanda, dos eventos identificados como exploits.

2.4.183. Deve permitir a atualização e desinstalação do agente a partir da console de gerenciamento.

2.4.184. Deve permitir o uso de qualquer aplicativo de terceiros para poder instalar o agente.

2.4.185. Deve possuir integração com o Active Directory para gerenciamento do computador e

configuração de políticas.

2.4.186. Deve ter a capacidade de criar perfis granulares.

2.4.187. Deve ter a capacidade de criar políticas com base nos grupos de máquinas criados.

2.4.188. Deve ter a capacidade de aplicar políticas a usuários, grupos, computadores ou unidades organizacionais do Active Directory.

2.4.189. Deve ter a capacidade de criar grupos virtuais que podem ser alimentados de forma estática e dinâmica.

2.4.190. Cada evento de prevenção ou alerta deve possuir informações básicas como tipo de evento, módulo que realizou a prevenção, detalhes daquele módulo, nome do computador, nome de usuário, sistema operacional, versão do agente, processo que gerou o evento de prevenção, rota de execução do processo que gerou o evento de prevenção (se disponível), hora e data do evento, informação forense (se disponível).

2.4.191. Deve ser fornecido sob um licenciamento de software como serviço (SaaS).

2.4.192. Deve possuir um dashboard mostrando os incidentes de segurança que não foram atendidos (classificados de acordo com sua criticidade em alta, média e baixa), um resumo dos incidentes de segurança, o número de endpoints que possuem o agente instalado (classificado para sua plataforma) e a versão do agente.

2.4.193. Deve possuir um dashboard onde são descritas as características dos incidentes de segurança que foram gerados. Este dashboard deve permitir uma análise mais detalhada dos alertas de segurança.

2.4.194. Deve permitir a criação de exceções a regras, mecanismos de detecção e/ou mecanismos de proteção a partir do console. Essas exceções devem ser aplicáveis a um computador específico ou a um grupo de computadores.

2.4.195. Características do Agente

2.4.196. Agente com footprint mínima que não afeta a experiência do usuário.

2.4.197. Pouco armazenamento em disco devido ao fato de não utilizar assinaturas, padrões e/ou heurísticas.

2.4.198. Suporte para as seguintes versões de sistemas operacionais:

2.4.199. Windows 7 (32-bit, 64-bit), Windows 8* (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows Embedded 8.1 Pro, Windows 10 Pro (32-bit and 64-bit), Windows 10 Enterprise LTSB,

Windows 10 Education, Windows 10 Update 1809, Windows Server 2003* (32-bit, SP2 o posterior), Windows Server 2003 R2 (32-bit, SP2 o posterior), Windows Server 2008 (32-bit, 64-bit; FIPS mode), Windows Server 2008 R2, Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 Datacenter, Windows Server 2019 Standard (Server Core), Windows Server 2022.

2.4.200. OSX 10.10 (Yosemite), OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.13.

2.4.201. CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16, Ubuntu Server 18, Ubuntu Server 20, Ubuntu 22.04 LTS.

2.4.202. Suporte a instalação de agente em serviços de gerenciamento de containers em nuvem como: Google Kubernetes (GKE), Amazon Elastic Kubernetes Services (EKS) e Azure Kubernetes Services (AKS); (Cloud per host)

2.4.203. A console deve permitir a criação do arquivo do agente de acordo com o sistema operacional;

2.4.204. Através da solução dOe gerência, deve ser possível verificar qual versão do agente está aplicada para determinado computador;

2.4.205. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: Agrupar máquinas com o mesmo sistema operacional, agrupar máquinas no mesmo range de IP, Agrupar máquinas com a mesma OU no Active Directory, etc;

2.4.206. Threat Hunting

2.4.207. Deve permitir pesquisar, agendar e salvar consultas para identificar ameaças.

2.4.208. Deve oferecer recursos de busca flexíveis que permitam descobrir ameaças usando um construtor de consultas intuitivo, além de criar consultas avançadas e exibir resultados de maneira ordenada.

2.4.209. Deve contextualizar automaticamente as ameaças usando inteligência de ameaças

2.4.210. Deve criar regras personalizadas de detecção de pesquisa de produtos e procurar manualmente por adversários emergentes usando os recursos de exploração de dados do produto;

2.4.211. Deve investigar ameaças e determinar o escopo completo dos incidentes.

2.4.212. Deve produzir relatórios detalhados de ameaças que revelam ferramentas de ataque e etapas para erradicar os adversários rapidamente.

2.4.213. Receber informações dos endpoints (Telemetria), de processos, comandos executados na maquina, informações de usuário e senha, mesmo antes da ocorrência de uma alerta ou incidente.

2.4.214. Possibilidade de criar relatórios e dashboards com base em informações específicas do cliente, além do padrão da ferramenta.

2.4.215. Deve oferecer assistência direta para responder a perguntas e fornecer orientação sobre relatórios de ameaças e relatórios de impacto.

2.4.216. No momento de investigação é de extrema importância a visibilidade da cadeia de todo o incidente, sendo que a gerência centralizada deverá apresentar o fluxo do ataque através de interface gráfica, detalhando os dispositivos envolvidos estando ele on premises ou em cloud pública;

2.4.217. A gerência centralizada através de sua interface gráfica, deverá apresentar os usuários e seus devidos níveis de riscos cibernéticos. Este nível de risco é calculado no volume de alertas, incidentes e características técnicas do usuário;

2.4.218. A gerência centralizada através de sua interface gráfica, deverá apresentar os usuários e seus devidos níveis de riscos cibernéticos através de uma linha de tempo que pode ser configurado data de início e fim para análises de comportamento.

2.4.219. Deve identificar e apresentar graficamente através de console centralizada, tentativa de descoberta da senha do usuário (ex.:Brute Force) quando integrado com servidores de domínio Active Directory.

2.4.220. Dashboard e Relatório

2.4.221. A solução deve ter a capacidade de consulta das informações de telemetria e logs permitindo a criação de dashboards e relatórios customizados.

2.4.222. Deve permitir a geração de relatórios sob demanda ou agendados.

2.4.223. O formato dos relatórios gerados deve ser em PDF.

2.4.224. Deve-se manter um histórico dos relatórios gerados para consulta posterior.

2.4.225. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

2.4.226. Deve permitir a configuração de uma frequência para geração dos relatórios programados, podendo ser diária, semanal ou mensal.

2.4.227. Se a frequência de geração de relatórios for semanal, deve poder especificar o dia em que os relatórios serão gerados.

2.4.228. Se a frequência de geração de relatórios for mensal, o relatório deverá ser gerado no dia selecionado de cada mês.

2.4.229. O intervalo de tempo para geração de relatórios deve ser expresso em dias.

2.4.230. Vários endereços de e-mail podem ser especificados para envio de relatórios.

2.4.231. Para relatórios sob demanda, o intervalo de tempo a ser considerado deve ser especificado.

2.4.232. Os relatórios podem ser gerados a partir de modelos predeterminados ou um relatório personalizado pode ser gerado usando os widgets disponíveis.

2.4.233. Deve ser possível a criação de widgets customizados a partir de pesquisa aos dados armazenados no Data Lake;

2.4.234. Os relatórios podem ser enviados para uma lista de e-mail.

2.4.235. A solução deve ter a capacidade de armazenar telemetria dos endpoints por 30 dias;

2.4.236. Gestão de ativos:

2.4.237. A solução de XDR deve possuir uma arquitetura onde deve não só apresentar informações do host que foi instalado o agente do XDR, mas também trazer visibilidade do dispositivo ao, mesmo ele não tendo instalado o agente do XDR.

2.4.238. A solução deve possuir um mecanismo de fazer o inventário dos computadores que possuem o agente instalado;

2.4.239. A solução deve fazer varredura na rede e apresentar através da gerência centralizada todos os dispositivos de rede mesmo não possuindo o agente do XDR instalado. Na visibilidade da console deverá intitular os dispositivos que possuem os agentes XDR instalados e os dispositivos que não possuem o XDR. Caso o fabricante não tenha essa capacidade na solução nativa, será permitida a composição com ferramentas de mercado do tipo NDR.

2.4.240. Para os dispositivos que não possuem o agente do XDR e que foram apresentados na console de gerência centralizada, devem apresentar as seguintes informações:

2.4.241. Endereço IP;

2.4.242. Range de IP;

2.4.243. Dispositivos on-premises ou virtual em cloud pública;

2.4.244. Dia/horário da primeira e da última detecção.

2.4.245. Caso o fabricante não tenha essa capacidade na solução nativa, será permitida a composição com ferramentas de mercado do tipo NDR.

2.4.246. As soluções dos itens 1, 2 e 3 deverão ser do mesmo fabricante, para que trabalhem de forma integrada.

2.4.247. Garantia mínima de 36 (trinta e seis) meses incluindo todas as licenças necessárias para as funcionalidades

2.5. ITEM 04: SOLUÇÃO DE ZERO TRUST NETWORK ACCESS (ZTNA) COM CAPACIDADE PARA SUPORTAR 200 USUÁRIOS - 36 MESES.

2.5.1. A solução de segurança na borda deverá suportar, no mínimo, as seguintes funcionalidades:

2.5.2. ZTNA (Zero Trust Network Access);

2.5.3. Filtro de URL;

2.5.4. Controle de Aplicação;

2.5.5. Prevenção de Ameaças;

2.5.6. Solução de segurança DNS;

2.5.7. Proteção Contra Malwares Modernos (Sandbox);

2.5.8. Gerência e Relatórios.

2.5.9. A solução deverá ser licenciada para permitir a autenticação para acesso de 200 usuários conectados simultaneamente

2.5.10. A solução disponibilizada deverá ter capacidade de receber via redirecionamento ou interceptar

de maneira ativa e realizar inspeção e tratamento de todo o tráfego web de forma a controlar os acessos a serviços SaaS (Gerenciados e não gerenciados), IaaS, Web e Aplicações Internas (Nuvem pública e on-premises).

2.5.11. A solução deve possuir console única de gestão para toda a plataforma de segurança, incluindo:

2.5.12. Painel de Política;

2.5.13. Painel de Relatório;

2.5.14. Painel de Incidentes;

2.5.15. Painel de Configuração;

2.5.16. Painel Analítico.

2.5.17. O fabricante da solução deverá possuir ao menos 2 gateways no Brasil com pelo menos 2 (dois) endereços IPs dedicados para cada um deles e garantir que as configurações sejam aplicadas aos mesmos localmente, não sendo permitidas soluções genéricas agregadas através de appliances físicos e/ou virtuais;

2.5.18. A solução deverá prover às redes remotas faixas de endereços exclusivos para acesso à Internet, saindo apenas com IPs designados para o Brasil.

2.5.19. Esta funcionalidade também deverá garantir que a mesma faixa de endereço não seja compartilhada com outros clientes;

2.5.20. Deverá ser fornecida com no mínimo, 2 (duas) estruturas de processamento redundantes no território nacional (Brasil)

2.5.21. A infraestrutura operacional do fabricante da solução deverá ter as certificações SOC-2 e ISO 27001

2.5.22. Deverá ser possível realizar a interceptação do tráfego de várias maneiras distintas, com o intuito de cobrir todo o escopo de alcance aos usuários, para no mínimo as seguintes formas:

2.5.23. Túnel Seguro (IPSEC ou SSL);

2.5.24. Integração com plataformas de SDWAN;

2.5.25. Integração com NGFW/UTM (IPSEC);

2.5.26. Agente (Windows, Linux e MacOS);

2.5.27. Os serviços de segurança devem ser fornecidos de maneira transparente às redes/usuários remotas;

2.5.28. A solução deve fornecer a capacidade de associar e atribuir toda a atividade do usuário, usando uma representação de identidade conforme integrações com:

2.5.29. Active Directory;

2.5.30. Federação (SSO) utilizando SAML v2.0;

2.5.31. OpenID Connect/OAuth 2.0;

2.5.32. A solução deverá ser capaz de prover acesso às aplicações internas sem a necessidade de instalação de máquinas virtuais na rede de destino como ponte de acesso;

2.5.33. A solução deverá executar suas funcionalidades para defender a rede/usuário contra ameaças avançadas, vírus e ameaças escondidas em tráfego HTTPS e aplicações com SSL criptografado;

2.5.34. A solução deverá ser capaz de descriptografar e inspecionar todo o tráfego SSL/TLS, nas versões TLS 1.2 ou superior;

2.5.35. O tráfego SSL/TLS deve ser inspecionado pelas mesmas políticas de filtragem aplicadas ao

tráfego não criptografado;

2.5.36. Deverá permitir a configuração de portas diferentes das portas padrão utilizadas pelos protocolos HTTPS/SSL e HTTP, utilizado no acesso de clientes a sites;

2.5.37. A solução deverá verificar os certificados digitais de sites acessados por meio do protocolo HTTPS.

2.5.38. Deverá permitir configurar regras de exceção a sites HTTPS que não devem ter seu tráfego inspecionado;

2.5.39. O licenciamento e a garantia pelo fabricante para toda a solução deverão estar ativos durante toda a vigência do contrato

2.5.40. ZTNA (Zero Trust Network Access)

2.5.41. A solução deve possuir a capacidade de controlar o acesso e aplicar controle de aplicação, proteção contra malwares modernos (Sandbox), prevenção de ameaças e segurança de DNS, de usuários remotos a aplicações internas através da nuvem do fabricante, onde o usuário remoto tenha acesso apenas a aplicação especificada na política de segurança e não a um segmento de rede interna;

2.5.42. A solução deve ser implementada com agente único na estação de trabalho do usuário remoto;

2.5.43. Ao se conectar remotamente na solução para acesso a uma aplicação interna, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

2.5.44. A solução deve garantir acesso seguro a nível de aplicação, ao invés de prover acesso local a rede;

2.5.45. Ser possível configurar através da console gráfica da solução quais aplicações internas serão

acessadas através do Tenant da solução;

2.5.46. Ser auto suficiente e se ajustar automaticamente do ponto de vista de performance caso algum ponto de presença venha a falhar sem a necessidade do administrador ou cliente configurar nenhuma regra;

2.5.47. Trabalhar em modo híbrido, onde seja possível publicar os atalhos de acesso a aplicações presentes nos datacenters e nas nuvens públicas indicadas;

2.5.48. A solução deve permitir definir a conformidade de estações com sistemas operacionais Windows, Linux e MacOS, com as políticas organizacionais baseadas no mínimo nos seguintes critérios:

2.5.49. Presença de processo(s) em execução;

2.5.50. Presença de arquivos em disco;

2.5.51. Participação em domínio do AD;

2.5.52. Existência de Certificado Digital no dispositivo;

2.5.53. Que somente as máquinas que estejam com solução anti-malware ativada possam acessar os serviços internos.

2.5.54. O cliente SSL client-to-site também deve suportar dispositivos móveis (IOS e ANDROID), sistemas operacionais Linux;

2.5.55. A solução deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

2.5.56. Máquinas em conformidade: A partir de uma máquina remota, com pré-requisitos de segurança identificados, deve permitir o acesso a aplicação;

2.5.57. Geolocalização: A partir de uma máquina remota tentando se conectar de um país não permitido, deverá ter sua conexão bloqueada;

2.5.58. Pela solução deve ser possível criar políticas de segurança onde pode ser especificado:

2.5.59. Usuário do AD;

2.5.60. Grupo do AD;

2.5.61. Aplicação Privada;

2.5.62. Perfil de segurança (por exemplo: Filtro de URLs, Controle de Aplicação e inspeção Anti-malware);

2.5.63. Ação: Permitir e/ou Bloquear.

2.5.64. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, chaves de registros e processos ativos;

2.5.65. A solução deve realizar verificação contínua de confiança, onde uma vez que o acesso a um aplicativo é concedido;

2.5.66. A confiança deverá ser continuamente avaliada com base em mudanças nas condições de segurança na estação;

2.5.67. Possuir capacidade de analisar dinamicamente (continuamente) os acessos dos usuários conectados remotamente a internet e recursos do próprio órgão;

2.5.68. Suportar políticas de permissão e negação de acesso com base em várias condições. Por exemplo: postura do dispositivo, localização do dispositivo/usuário, associação ao grupo de usuários;

2.5.69. Se algum comportamento suspeito for detectado, o acesso pode ser revogado em tempo real;

2.5.70. A solução deve gerar logs dos acessos realizados por usuários remotos as aplicações internas, no mínimo, com as seguintes informações:

2.5.71. Regra de segurança que foi aplicada no tráfego;

2.5.72. Ação tomada pela solução;

2.5.73. Usuário;

2.5.74. Endereço IP;

2.5.75. IP público e IP privado.

2.5.76. País de origem;

2.5.77. Porta de origem;

2.5.78. Sistema operacional;

2.5.79. Aplicação de destino;

2.5.80. Porta de destino;

2.5.81. Protocolo;

2.5.82. Bytes trafegados na sessão;

2.5.83. Hora de início e término da sessão.

2.5.84. Deve permitir que a conexão com o serviço SASE seja estabelecida das seguintes formas:

2.5.85. Antes do usuário autenticar na estação;

2.5.86. Após autenticação do usuário na estação;

2.5.87. Sob demanda do usuário;

2.5.88. Sempre ativo mantendo o usuário conectado assim que o usuário faz o logon.

2.5.89. A solução deve enviar a lista de gateways ativos para estabelecimento da conexão;

2.5.90. Deve haver a opção do cliente remoto escolher manualmente o gateway de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

2.5.91. FILTRO DE URLS

2.5.92. A solução deverá suportar a criação de políticas baseadas no controle por URL e categorias de URLs;

2.5.93. O perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

2.5.94. A solução deverá possuir:

2.5.95. Pelo menos 70 categorias distintas de URLs;

2.5.96. A capacidade de classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

2.5.97. Categoria específica para classificar domínios recém registrados (com menos de 30 dias);

2.5.98. Base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;

2.5.99. A solução deve possuir, no mínimo, os seguintes atributos para construção de políticas de filtro de conteúdo WEB:

2.5.100. Categoria de URL;

2.5.101. Usuários e Grupos do Active Directory;

2.5.102. Profile de prevenção de malwares;

2.5.103. Atividade realizada na URL/Aplicação;

2.5.104. IP de Origem;

2.5.105. IP de Destino;

2.5.106. País de origem e destino;

2.5.107. Ação: allow, block e alert;

2.5.108. Tipo de arquivo.

2.5.109. A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório;

2.5.110. A solução deverá suportar:

2.5.111. A criação de categorias de URLs customizadas;

2.5.112. A exclusão de URLs do bloqueio, por categoria;

2.5.113. A customização de página de bloqueio;

2.5.114. A capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local.

2.5.115. A solução deverá permitir:

2.5.116. Um mecanismo para sobrescrever as categorias de URL;

2.5.117. A criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

2.5.118. Especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

2.5.119. A solução deverá possuir mecanismo de Controle de URL que apresenta contagem de utilização de regra de acordo com a utilização (hit count);

2.5.120. A solução deverá possibilitar:

2.5.121. Categorização e recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

2.5.122. A inspeção de tráfego HTTPS Outbound deverá efetuar o "man-in-the-middle", ou seja, a solução deverá prover mecanismo de descriptografia para inspeção completa do tráfego de saída para a internet;

2.5.123. Implementação de filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das estações dos clientes.

2.5.124. O cadastro manual de usuários e grupos diretamente na interface de gerência remota;

2.5.125. O bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

2.5.126. Salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

2.5.127. A solução deverá ser capaz de detectar e prevenir roubo de credenciais, controlando e

bloqueando os sites que o usuário pode enviar credenciais corporativas com base na classificação do endereço, em tempo real.

2.5.128.A solução deverá possuir a capacidade de detectar técnicas de phishing ou falsificação de imagens;

2.5.129.A solução deverá utilizar modelos de inteligência preditiva no reconhecimento de URLs maliciosas em tempo real não cadastradas na base de categorização do fabricante da solução.

2.5.130.CONTROLE DE APLICAÇÕES

2.5.131.A solução deverá possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.5.132.A solução deverá contar com módulos de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;

2.5.133.Pela solução deverá ser possível:

2.5.134.A liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;

2.5.135.A criação de políticas por geolocalização, permitindo que o tráfego de uma aplicação para um determinado país seja bloqueado ou redirecionado;

2.5.136.Adicionar políticas de controle de aplicações e perfis de segurança para todo o tráfego web e interno através da nuvem SSE, não se limitando somente a possibilidade de habilitar controle de aplicações em parte do tráfego;

2.5.137.Adicionar controle de aplicações em todas as regras de segurança da solução, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

2.5.138. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do AD;

2.5.139. A criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

2.5.140. Nível de risco da aplicação;

2.5.141. Categoria de aplicações.

2.5.142. A solução deverá reconhecer pelo menos 3.000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e webmail;

2.5.143. A solução deverá suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos assinaturas, decoders de protocolos e heurísticas;

2.5.144. A solução deverá diferenciar:

2.5.145. Tráfegos peer-to-peer (bittorrent, emule, neonet, etc.), possuindo granularidade de controle para os mesmos;

2.5.146. Tráfegos de mensageiros instantâneos (facebook Chat, WhatsApp, telegram e etc.) possuindo granularidade de controle para os mesmos;

2.5.147. Aplicações proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle para eles.

2.5.148. A solução deverá diferenciar e controlar partes das aplicações, incluindo, mas não limitado: Permitir o WhatsApp WEB e bloquear a transferência de arquivos, permitir o facebook e bloquear chat;

2.5.149. Pela solução deverá ser possível:

2.5.150. Inspecionar o payload do pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

2.5.151. Realizar filtragens/inspeções dentro de portas TCP conhecidas, por exemplo porta 80 http, buscando por aplicações que potencialmente expõem o ambiente como: peer-to-peer ou mensageiros instantâneos;

2.5.152. Identificar o uso de táticas evasivas, ou seja, deverá ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como ataques utilizando comunicação TLS;

2.5.153. Aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a encrypted bittorrent e aplicações VOIP que utilizam criptografia proprietária.

2.5.154. Caso a solução não tenha assinaturas pré-definidas de uma aplicação, ela deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, HTTPS, FTP, E-mail e extensão de arquivos;

2.5.155. Pela solução deverá ser possível atualizar a base de assinaturas de aplicações automaticamente;

2.5.156. O fabricante da solução deverá disponibilizar um serviço para solicitação de inclusão de aplicações na base de assinaturas dele;

2.5.157. PREVENÇÃO DE AMEAÇAS.

2.5.158. A solução deverá proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto à movimentação entre nuvens (SaaS Gerenciado e SaaS não gerenciado);

2.5.159. Na solução deverá ser possível criar políticas de segurança baseadas no nível de risco da aplicação. Ex: selecionar na política de segurança o bloqueio de todas as aplicações de cloud storage com nível de risco alto na base do fabricante da solução;

2.5.160. Deve conter, no mínimo, as seguintes informações sobre as aplicações comparadas na interface gráfica da solução:

2.5.161. Informações sobre vulnerabilidades e exploits já sofridos;

2.5.162. Certificações e normas que a aplicação está aderente. Ex: PCI, DSS, SOC-1, SOC-2 e SOC-3;

2.5.163. Informações sobre privacidade de dados. Ex: ao armazenar dados na aplicação, o cliente continua sendo proprietário dos dados.

2.5.164. A solução deverá possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

2.5.165. A solução deverá suportar:

2.5.166. Várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

2.5.167. Referência cruzada com CVE.

2.5.168. A solução deverá ser capaz de categorizar os seguintes tipos de domínio:

2.5.169. Domínios de DNS dinâmicos;

2.5.170. Domínios identificados previamente como sendo distribuidores de Malwares;

2.5.171. Domínios identificados anteriormente em campanhas de Phishing;

2.5.172. Domínios identificados previamente como Graywares os quais podem usar de técnicas de instalação de aplicações não desejadas;

2.5.173. Domínios Estacionários os quais são sites com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares;

2.5.174. Domínio de anonimização de Proxy utilizados com uma forma de driblar a análise de conteúdo.

2.5.175. A solução deverá possuir sistema de análise automática para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.5.176. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos;

2.5.177. A solução deverá permitir updates em tempo real para ameaças e novos ataques feitos através de DNS.;

2.5.178. SOLUÇÃO DE SEGURANÇA DNS

2.5.179. A solução de segurança de DNS, tem como finalidade proteger as conexões a domínios maliciosos que muitas vezes são utilizados pelos atacantes, utilizam para interceptar a comunicação e poder ter acesso e controlar a comunicação dos usuários, causando problemas de evasão e exfiltração de dados;

2.5.180. Caso o fabricante não tenha solução de segurança para DNS de forma nativa, ou seja, licenciada de forma separada da solução, o mesmo pode compor com outra solução dedicada de mercado de fabricantes como (ex.: Cisco Umbrella) e deverá ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

2.5.181. A solução de segurança de DNS deve ser capaz de identificar atividades maliciosas de comando e controle utilizado pelo menos as seguintes técnicas:

2.5.182. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

2.5.183. Domínio suspeito identificado;

2.5.184. ID de assinatura de detecção;

2.5.185. Usuário logado na estação/servidor que originou o tráfego;

2.5.186. Aplicação;

2.5.187. Porta de destino;

2.5.188. IP de origem;

2.5.189. IP de destino;

2.5.190. Horário;

2.5.191. Ação do firewall;

2.5.192. Severidade;

2.5.193. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.5.194. A análise automática deve incluir, no mínimo, as seguintes características:

2.5.195. Padrões de consulta;

2.5.196. Entropia;

2.5.197. Análise de frequência n-gram de domínios;

2.5.198. Taxa de consultas.

2.5.199. A solução deve permitir updates em tempo real para ameaças e novos ataques feitos através de DNS;

2.5.200. A solução deve permitir a utilização ilimitada (quantidades) de assinaturas DNS;

2.5.201. A solução de segurança de DNS deve ser capaz de categorizar os seguintes tipos de domínio:

2.5.202. Domínios de DNS dinâmicos

2.5.203. Domínios identificados previamente como sendo distribuidores de malwares

2.5.204. Domínios registrados recentemente

2.5.205. Domínios identificados anteriormente em campanhas de phishing

2.5.206. Domínios identificados previamente como graywares os quais podem usar de técnicas de instalação de aplicações não desejadas

2.5.207. Domínios Estacionários os quais são sítios com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares.

2.5.208. Domínio de proxy de animação utilizados com uma forma de driblar a análise de conteúdo.

2.5.209. PROTEÇÃO CONTRA MALWARES MODERNOS

2.5.210. A solução deverá possuir nuvem de inteligência proprietária do fabricante que seja responsável em atualizar toda a base de segurança através de assinaturas;

2.5.211. A solução deve ser capaz de enviar arquivos trafegados de forma automática para análise em tempo real em uma sandbox, devendo permitir a análise na nuvem do fabricante da solução, onde o arquivo será executado e simulado em ambiente controlado (sandbox). Caso esta funcionalidade seja licenciada de forma separada da solução, deverão ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

2.5.212. A solução deverá prevenir o uso de exploits avançados;

2.5.213. Na solução, a análise deverá prover:

2.5.214. Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

2.5.215. Informações sobre as ações do malware na máquina infectada;

2.5.216. Informações sobre as URLs não confiáveis utilizadas pelo novo malware;

2.5.217. Informações sobre quais aplicações são utilizadas para causar/propagar a infecção;

2.5.218. Detecção de aplicações não confiáveis, utilizadas pelo Malware;

2.5.219. Assinaturas de antivírus e antispyware de maneira automática.

2.5.220. A solução deverá possuir:

2.5.221. Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS;

2.5.222. Mecanismo de detecção "antibot", que inclui pelo menos, reputação de endereço IP;

2.5.223. Funcionalidade de detecção e bloqueio de call-backs.

2.5.224. A solução deverá prevenir contra ameaças de dia zero:

2.5.225. Via tráfego de internet;

2.5.226. Que possam burlar o sistema operacional emulado;

2.5.227. Através de tecnologias em nível de emulação e código de registro.

2.5.228. A solução deverá ser capaz de implementar:

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

2.5.230. Visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

2.5.231. Análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

2.5.232. A solução deverá suportar ainda:

2.5.233. Identificação e bloqueio de malware nas comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

2.5.234. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

2.5.235. Suportar a análise dinâmica de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows 10, Mac OS X, iOS, Android e Linux;

2.5.236. A solução deve analisar os arquivos do tipo malware em bare-metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função;

2.5.237. Serviço de Instalação e Suporte

2.5.238. O fabricante deverá em conjunto com a contratante realizar atividades de planejamento e uma call de Kick-off para realizar o lançamento inicial do projeto. Esta reunião discutirá o seguinte:

2.5.239. Conexões de serviço;

2.5.240. Usuários móveis.

2.5.241. Após o kick-off, a Contratada em conjunto com o fabricante deverá gerar um Documento de Requisitos Técnico, baseado no ambiente do cliente

2.5.242. O Documento de Requisitos Técnicos descreverá o ambiente de produção planejado e os procedimentos operacionais, incluindo a integração de conexões de serviço, redes remotas e usuários móveis que foram acordados durante o kick-off

2.5.243. A Contratada em conjunto com o fabricante deverá:

2.5.244. Realizar o envio do Documento de Requisitos Técnicos para que a Contratante revise em até 5 cinco dias úteis para aprovação. Se necessário, a Contratada deverá organizar com o fabricante uma nova reunião de revisão do documento

2.5.245. Realizar a configuração com base nos requisitos definidos no Documento de Requisitos Técnicos. As tarefas de configuração devem incluir no mínimo:

2.5.246. Configuração da licença, download e instalação do plug-in de serviços em nuvem;

2.5.247. Duas (2) conexões de serviços;

2.5.248. Um (1) túnel IPSec para o site principal da contratante;

2.5.249. Um (1) túnel IPSec para a unidade remota a escolha da contratante;

2.5.250. Configuração do roteamento dinâmico/estático;

2.5.251. Um (1) portal de a integração de usuários móveis;

2.5.252. Configuração do pool de IPs para os usuários móveis;

2.5.253. Onboard de usuários móveis;

2.5.254. Dez (10) políticas de segurança;

2.5.255. Assistência em testes;

2.5.256. Um (1) perfil de autenticação em um serviço externo.

2.5.257. Revisará e validar a implantação de acordo com os critérios definidos no Documento de Requisitos Técnicos;

2.5.258. Realizar uma sessão de transferência de conhecimento após a conclusão dos serviços de planejamento, configuração e validação listados acima;

2.5.259. Realiza uma sessão de Transferência de Conhecimento deverá incluir uma descrição do ambiente as-built e uma transferência de informações sobre como gerenciar e operar o ambiente. A transferência de conhecimento deverá ser realizada em uma única sessão de até duas (2) horas, para oito (8) participantes;

2.5.260. Em até quinze (15) dias depois da etapa de validação, realizar o ajuste final do ambiente e As-Built

2.5.261. O Serviço de suporte deverá valer durante toda a vigência contratual de 36 (trinta e seis) meses:

2.5.262. Abertura de chamados através de telefone diretamente com o fabricante no modelo 24x7;

2.5.263. Abertura de chamados através de portal diretamente com o fabricante no modelo 24x7.

2.5.264. Acesso a Especialistas Técnicos e Recursos Online:

2.5.265. A solução deverá fornecer acesso imediato a especialistas técnicos e recursos online, garantindo proteção ao produto oferecido. Os usuários poderão submeter, atualizar e verificar o status dos casos de suporte por meio de um Portal de Suporte ao Cliente online.

2.5.266. Transferência de Conhecimento Avançada:

2.5.267. A solução incluirá uma plataforma completa de transferência de conhecimento. Isso abrangerá documentação detalhada do produto, bancos de dados de resolução de problemas e um ambiente de gerenciamento de casos de suporte baseado em conhecimento, permitindo colaboração entre usuários. Além disso, serão disponibilizados manuais de produtos, guias técnicos, notas de lançamento de software e FAQs para simplificar a resolução de incidentes.

2.5.268. Serviço de Melhoria Contínua:

2.5.269. A solução oferecerá um serviço de melhoria contínua para maximizar o valor do produto. Isso incluirá o desenvolvimento de planos de sucesso personalizados, alinhados com metas e requisitos específicos da organização. Serão realizadas verificações periódicas da saúde da solução e aplicadas as melhores estratégias de utilização para otimização e proteção do investimento.

2.5.270. Integração de Fluxos de Trabalho Operacionais:

2.5.271. A solução garantirá a integração eficaz com fluxos de trabalho operacionais. A equipe especializada colaborará com a infraestrutura de rede e segurança, identificando pontos de integração, conduzindo verificações regulares e revisões operacionais para promover uma operação mais eficiente e aumentar a confiança na solução.

2.5.272. Garantia mínima de 36 (trinta e seis) meses incluindo todas as licenças necessárias para as funcionalidades

2.6. ITEM 06: SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DA SOLUÇÃO

2.6.1. Garantia e Suporte:

2.6.2. Garantia mínima de 36 (trinta e seis) meses, Onsite, fornecida pelo FABRICANTE e CONTRATADA, com suporte técnico 24/7 para hardware e software;

2.6.3. A LICITANTE deverá informar na proposta o tipo e o período da garantia. No momento da análise da proposta será verificado junto ao FABRICANTE da solução, através de consulta, a

disponibilidade de oferta da garantia e no momento da entrega do equipamento também será verificado o prazo on-site;

2.6.4. Os serviços serão solicitados mediante a abertura de chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português) e constatada a necessidade, a Empresa Licitante deverá providenciar o deslocamento do equipamento, peças ou partes, bem como seu retorno ao local de origem e ainda do técnico responsável para solução do problema no local, sem qualquer ônus ao contratante;

2.6.5. Deverão ser fornecidas as atualizações corretivas e evolutivas do software durante o período de garantia;

2.6.6. Quanto às atualizações pertinentes aos softwares, entende-se como "atualização" o provimento de toda e qualquer evolução de software, oficial e comprovadamente disponibilizada pelo fabricante da solução, incluindo correções, "patches", "fixes", "updates", "service packs", novos "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas e, deverá ser revisada a cada semestre;

2.6.7. Durante a vigência da garantia, o atendimento remoto do fabricante do appliance deve permitir, sem limite de quantidade, que a assistência remota realize, pelo menos, as seguintes tarefas:

2.6.8. Instalação de correções e atualizações;

2.6.9. Revisão das configurações e sugestão de melhores práticas do fabricante;

2.6.10. Reconfiguração e reinstalação do appliance, caso seja for necessário.

2.6.11. A CONTRATADA deverá fornecer juntamente com a solução o acesso expresso ao 2º nível de atendimento do fabricante, ou seja, nível onde o analista de suporte é qualificado para atuar diretamente no problema, sem necessidade de triagem prévia. O analista de suporte do fabricante deve, adicionalmente, realizar durante todo o período de garantia as seguintes atividades:

2.6.12. Verificações proativas junto ao CONTRATANTE, esclarecimento de dúvidas.

2.6.13. O serviço deverá estar disponível, em conformidade com nosso NMQS (Nível Mínimo de Qualidade de Serviço), dentro dos padrões de qualidade, disponibilidade e desempenho estipulados a seguir:

2.6.14. Nível de Acordo de Serviço: 24x7

2.6.15. A assistência técnica deverá estar disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

2.6.16. **NÍVEIS MÍNIMOS DE QUALIDADE DE SERVIÇO**

2.6.17. Os chamados de suporte técnico serão classificados por níveis de severidade de acordo como impacto no ambiente computacional da contratante, de acordo com as tabelas abaixo de Níveis de Severidade:

Nível	Descrição do Impacto
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Serviços disponíveis com ocorrência de alarmes de avisos
4	Dúvidas informacionais sobre as soluções vinculadas ao contrato

Prazos de Atendimento

Níveis de Severidade dos Chamados	Prazo	Níveis de Severidade			
Modalidade de Atendimento		1	2	3	4
Remoto	Início do Atendimento	1 hora	12 horas	24 horas	48 horas
Remoto	Solução de Contorno	4 horas	12 horas	36 horas	72 horas

2.6.18. Instalação, configuração e passagem de conhecimento

2.6.19. Os serviços de instalação, implantação e configuração envolverão as seguintes etapas:

2.6.20. Descrição do plano de implantação;

2.6.21. Cronograma;

2.6.22. A CONTRATADA deve auxiliar a CONTRATANTE na atualização das políticas, apresentando as melhores práticas de mercado, as práticas que melhor se adequem a realidade da EMAP e de uso dos softwares de cópias de segurança desta contratação.

2.6.23. O serviço de instalação do equipamento deverá contemplar, no mínimo, as seguintes atividades:

2.6.24. Desembalagem e inspeção dos equipamentos.

2.6.25. Conexão de cabos de energia e lógicos.

2.6.26. Instalação de correções de firmware, atualizando o produto fornecido para o último nível recomendado pelo fabricante.

2.6.27. Ativação das licenças/features adquiridas juntamente com o equipamento.

2.6.28. Migração de regras e políticas dos equipamentos antigos para os novos.

2.6.29. Após a conclusão da instalação da solução, um técnico da CONTRATADA deverá ser disponibilizado na EMAP por 03 (três) dias úteis consecutivos, virtual ou presencialmente, em data e hora a ser combinada com a CONTRANTE, entre 08h (oito horas) e 17h (dezoito horas), totalizando 24 (vinte e quatro) horas, para realizar os ajustes necessários e atender às demandas da equipe de infraestrutura de TI da EMAP, sem custos adicionais para a CONTRATANTE.

2.6.30. Serviço de instalação e configuração de firewall ngfw

2.6.31. A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

2.6.32. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

2.6.33. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);

2.6.34. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;

2.6.35. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

2.6.36. Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;

2.6.37. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

2.6.38. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;

2.6.39. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;

2.6.40. Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;

2.6.41. A instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos deverá ocorrer no Data Center a EMAP, em horário comercial, acordado previamente com a equipe da CONTRATANTE;

2.6.42. Ao final da implantação a contratada deverá fornecer a As Built da solução entregue, este documento deverá apresentar todo descritivo técnico da solução implantada, acls, integrações realizadas, funcionalidades ativadas, listas de interfaces físicas e logicas criadas, conexões físicas realizadas etc;

2.6.43. Todos os cabos de conexão, acessórios e itens relacionados ao completo funcionamento das soluções adquiridas devem ser fornecidos pela CONTRATADA.

2.6.44. Serviços de treinamento com profissional certificado pelo fabricante da solução

2.6.45. Repasse de conhecimento poderá ser feito presencial ou distância, via webconferência;

2.6.46. O treinamento deverá ser ministrado em português;

2.6.47. O material didático deverá estar em português e deverá ser disponibilizado em modo físico e digital;

2.6.48. Deverá ter carga horária mínima de 20 Horas;

2.6.49. O treinamento deverá conhecimentos de todas as funcionalidades da solução contratada, para instalação, administração, configuração, otimização, resolução de problemas e utilização da solução;

2.6.50. O treinamento compreenderá a transferência de conhecimento das tecnologias envolvidas na Solução de Segurança contratada, envolvendo, no mínimo, os seguintes itens:

2.6.51. Equipamento de Firewall:

2.6.52. Funcionalidade de Firewall;

2.6.53. Funcionalidade de QoS;

2.6.54. Funcionalidade de VPN;

2.6.55. Funcionalidade de Prevenção de Intrusão;

2.6.56. Funcionalidade de Filtragem WEB;

2.6.57. Funcionalidade de Prevenção de Ameaças;

2.6.58. Solução de Gerenciamento e Relatórios e suas funcionalidades;

2.6.59. Funcionalidade de Prevenção de Ameaças Avançadas (Sandbox) e suas funcionalidades;

2.6.60. Funcionalidades de DNS security and IoT security;

2.6.61. O treinamento da solução será no formato hands-on para a equipe responsável pelo projeto por parte da contratante após validação da migração;

2.6.62. O treinamento deve ser realizado em dias úteis, no horário das 08h às 12h e das 14h às 17h;

2.6.63. A CONTRATANTE deve se responsabilizar por qualquer material físico necessário para a execução dos treinamentos;

2.6.64. O serviço deverá ser ministrado por profissional certificado na solução de proteção de rede;

2.6.65. A contratada deverá apresentar, a nível de comprovação, os certificados do instrutor que ministrará o treinamento, os certificados deveram compreender, no mínimo, de administração da solução e de especialistas nela;

2.6.66. O serviço deverá ser baseado no treinamento oficial da solução contratada;

2.6.67. O certificado de conclusão deverá ser emitido em português brasileiro.

2.6.68. As aulas deverão ser gravadas e disponibilizadas a EMAP após o fim do treinamento.

3. JUSTIFICATIVA

Diante do cenário atual, marcado por uma evolução constante e crescente sofisticação das ameaças cibernéticas, torna-se imperativo para nós, na Empresa Maranhense de Administração Portuária (EMAP), reconhecer e reforçar a segurança da Tecnologia da Informação e Comunicação (TIC) como um pilar fundamental. Esta necessidade não apenas abrange a preservação da integridade, confidencialidade e disponibilidade de nossos recursos tecnológicos, mas também implica uma abordagem proativa e especializada para a segurança dos dados e sistemas críticos que sustentam nossa operação.

Atualmente, contamos com uma Solução de Firewall de Próxima Geração que tem atendido satisfatoriamente às nossas necessidades. Contudo, a descontinuação anunciada desse equipamento para dezembro de 2023 nos coloca diante de uma situação crítica, onde a falta de atualização poderá resultar na perda de suporte, garantia, e mais alarmante, na incapacidade de receber atualizações

críticas. Esta condição nos expõe a riscos substanciais, comprometendo a segurança de nossa rede e, por extensão, de toda a operação da EMAP.

A necessidade de atualização vai além da substituição de um equipamento; ela envolve a implementação de um sistema avançado que incorpore não apenas as funcionalidades tradicionais, mas também recursos aprimorados como filtragem de conteúdo, prevenção de intrusões e análise de comportamento. Estes recursos são essenciais para nos proteger contra ameaças avançadas, filtrar tráfego malicioso e impedir acessos não autorizados, servindo como a espinha dorsal da nossa defesa cibernética.

Além disso, a complexidade e sofisticação crescentes dos ataques cibernéticos exigem de nós uma abordagem integrada de segurança, que inclui a necessidade de um sistema de gerenciamento centralizado e integrado. Tal sistema permitirá administrar de forma centralizada todas as operações relacionadas à segurança, simplificando a administração e o monitoramento, além de automatizar as tarefas de instalação, configuração e atualização de soluções antimalware. Essa capacidade de automação é crucial para a eficácia de nossa defesa cibernética, facilitando a gestão de políticas de segurança, atualizações e relatórios, e garantindo maior eficiência operacional e consistência nas configurações.

A urgência dessa atualização é exacerbada pelo cenário atual de ciberataques, que não poupa nem empresas nem órgãos públicos. A segurança da informação é essencial para proteger nossos ativos organizacionais em um ambiente digital cada vez mais complexo. Portanto, a aquisição de uma ferramenta moderna e robusta é vital para prevenir vulnerabilidades, automatizar respostas a incidentes e centralizar o gerenciamento dos ativos de segurança.

A contratação proposta é indispensável também por ser capaz de atender às exigências críticas de segurança dos nossos sistemas de informação, visando proporcionar um acesso seguro aos Serviços de Rede hospedados em nossos servidores. Esta integração de uma solução de Firewall com detecção e resposta estendida é uma necessidade estratégica para fortalecer nossa postura defensiva e garantir a continuidade operacional frente às ameaças cibernéticas em constante evolução.

Em resumo, esta justificativa sublinha a necessidade premente de aprimorar nossa infraestrutura de segurança cibernética, não apenas para enfrentar os desafios imediatos impostos pela descontinuação de equipamentos críticos, mas também para nos posicionar de forma resiliente e proativa diante de um panorama de ameaças em evolução. A contratação das soluções descritas neste Termo de Referência não é apenas uma medida de fortalecimento de nossa defesa cibernética; é uma decisão estratégica para garantir a segurança robusta de nossa infraestrutura tecnológica e o resguardo de informações sensíveis contra ameaças cibernéticas.

4. PRAZOS DE VIGÊNCIA E EXECUÇÃO

4.1 O prazo de vigência de que trata esta contratação será de 15 (quinze) meses, devendo ser iniciado a partir da data de assinatura do contrato.

4.2 O prazo de execução contratual será de 12 (doze) meses, contando-se a partir da data indicada na Ordem de Fornecimento, a ser emitida pela EMAP, autorizando o início das atividades.

5. LOCAL DE FORNECIMENTO

5.1 Os objetos constantes deste termo deverão sem entregues na sede da Empresa Maranhense de Administração Portuária – EMAP. Porto do Itaqui, Avenida dos Portugueses s/nº. CEP 65085-370, São Luís-Maranhão, na sala da Gerência de Tecnologia e Informação, aos cuidados do Gerente ou Coordenador.

6. ENTREGA DOS PRODUTOS

6.1 - Prazo

A contratada terá o prazo de até 60 (Sessenta) dias corridos, contados a partir da data indicada na Ordem de Fornecimento, para concluir a entrega dos equipamentos

6.2 -Condições de recebimento

6.2.1 Os equipamentos somente serão recebidos pelo Fiscal se estiverem de acordo com as especificações deste Termo de Referência e na quantidade e forma estabelecidas na respectiva Ordem de Fornecimento.

6.2.2 A entrega deverá ser feita pela empresa vencedora em dias úteis, entre as 8h e 15h, sendo recebido pelo Fiscal do contrato.

6.2.3 O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato.

6.2.4 A assinatura do termo de aceite serve para subsidiar o recebimento provisório do objeto deste Contrato pela Fiscalização no prazo de até 05 (cinco) dias corridos contados da comunicação escrita do contratado, e definitivamente por servidor ou comissão designada pelo Presidente da EMAP, no prazo de até 30 (trinta) dias contados da comunicação escrita do contratado ou do recebimento provisório, mediante recibo.

6.3 -Cronograma

Os equipamentos serão entregues em lote único, em um prazo de até 60 (Sessenta) dias corridos, contados a partir da data indicada na Ordem de Fornecimento.

7. SAÚDE, SEGURANÇA, MEIO AMBIENTE E GETIN

RECOMENDAÇÕES GETIN:

- Os softwares a serem entregues deverão ser licenciados para EMAP;
- As licenças deverão ser, preferencialmente, perpétuas. Na impossibilidade de licenças perpétuas deverão estar licenciados para, pelo menos, 3 (três) anos;
- No licenciamento do software já deverá estar contemplado, pelo menos, 1 (um) ano de suporte mensal ao software junto ao fabricante.
- Este suporte deverá contemplar o fornecimento de atualizações, correções e versões.
- Acesso a portal para reclamações, dúvidas e abertura de chamados.
- PC 07 - 5.4 USO DE ATIVOS DE INFORMAÇÃO, Para todo ativo de informação, haverá um responsável e esse necessariamente deverá ser um funcionário da EMAP.

8. VALOR ESTIMADO E DISPONIBILIDADE FINANCEIRA

Disponibilidade Financeira

Para efeito de disponibilidade financeira o gasto foi previsto e será executado no centro de custo da Gerência de Tecnologia da Informação - GETIN, grupo de investimento CAPEX, subgrupo CAPEX TI, descrição dos investimentos:

- CAPEX 2024 - GETIN – FIREWALL

ITEM	DESCRIÇÃO	QUANTIDADE
1	Solução de Next Generation Firewall em Alta Disponibilidade	2
2	Solução de Gerenciamento Centralizado	1
3	Solução de detecção e resposta estendidas para estações de trabalho e servidores.	700
4	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 200 usuários - 36 meses	1
5	Serviço de instalação, configuração e migração da solução	1

Valor esse correspondente ao desembolso financeiro a ser efetuado no exercício orçamentário deste ano de 2024.

9. GESTÃO DA FISCALIZAÇÃO

O acompanhamento da execução do objeto deste Termo de Referência será gerenciado e fiscalizado por representantes do Contratante**, Ruan Louzeiro Santos** e nas suas ausências **Henrique Farias**, que poderão exigir da Contratada a qualquer tempo, esclarecimentos, demonstrações e documentos que comprovem a regularidade do contrato).

O fiscal do contrato terá poderes para:

a) Transmitir a CONTRATADA as determinações que julgar necessárias;

b) Recusar os serviços que não tenham sido realizados de acordo com as condições ajustadas;

c) Ordenar a imediata retirada de suas dependências, de empregados da CONTRATADA, cuja permanência seja inconveniente, ou que venha embaraçar ou

dificultar a ação fiscalizadora, correndo por exclusiva conta da CONTRATADAS quaisquer ônus decorrentes das leis trabalhistas e previdenciárias, bem como qualquer outra que tal fato imponha;

d) Acusar a falta de atendimento às solicitações das unidades por parte da CONTRATADA, bem como o atendimento inadequado, incompleto e/ou retardatário, notificando-a para que proceda à imediata regularização, sob pena de serem aplicadas as sanções e penalidades previstas neste instrumento e na lei;

e) Avaliar a qualidade dos serviços e fornecimentos e atestá-los quando em conformidade com os termos deste Termo e do contrato.

10. ANÁLISE DE RISCO PARA GARANTIA DE EXECUÇÃO DO CONTRATO

10.1 O Contratado prestará garantia em até 10 (dez) dias úteis após a assinatura do contrato, no percentual de 5% (cinco por cento) do valor global contratado, a qual se estenderá por 03 (três) meses após o término da vigência contratual, devendo ser renovada a cada prorrogação, em uma das modalidades a seguir, não sendo concedido, em nenhuma hipótese, prazo para apresentação da garantia após esse prazo:

- Caução em dinheiro;
- Seguro-garantia;
- Fiança bancária.

10.2 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

- prejuízos advindos do não cumprimento do contrato;
- Multas aplicadas ao Contratado;
- Prejuízos diretos causados à Contratante decorrentes de culpa ou de dolo durante a execução do contrato;
- Obrigações previdenciárias e trabalhistas não honradas pelo Contratado.

10.3 Se a opção de garantia for a caução em dinheiro, o Contratado deverá solicitar informações à EMAP referentes ao nome da instituição financeira, aos números da conta corrente e da

agência bancária, e ao código identificador, para efeito de depósito do crédito, sendo que o valor caucionado será restituído considerando-se os critérios vigentes de remuneração da poupança aplicados à época da devolução.

10.4 Se a opção recair em seguro-garantia, deverá ser feita a entrega da apólice em original, acompanhada de comprovante de pagamento do respectivo prêmio, devendo ainda conter expressamente cláusula de atualização financeira, de imprescritibilidade, inalienabilidade e de irrevogabilidade e deverá ser válida por pelo menos 90 (noventa) dias consecutivos após o prazo de validade deste contrato. A modalidade seguro garantia somente será aceita se contemplar todos os eventos indicados no parágrafo primeiro da cláusula décima deste Contrato.

10.5 Se a opção recair em fiança bancária, deverá ser feita a entrega da Carta de Fiança, em original, assinada pelo (s) representante (s) legal (is) do emitente devidamente comprovado, devendo conter expressamente cláusula de atualização financeira, de imprescritibilidade, inalienabilidade e de irrevogabilidade e deverá ser válida por pelo menos 90 (noventa) dias consecutivos após o prazo de validade do contrato.

10.6 Caso ocorra a prorrogação do Contrato, a Contratada fica obrigada a apresentar, no ato da assinatura do Termo Aditivo ou em até 10 (dez) dias úteis dessa data, a critério da EMAP, a renovação da caução prestada quando a mesma tiver sido feita nas modalidades de seguro garantia ou fiança bancária.

10.7 A Contratante poderá descontar do valor da garantia toda e qualquer importância que lhe for devida, a qualquer título, pelo Contratado, inclusive multas. Se o desconto se efetivar no decorrer do prazo contratual, a caução deverá ser reintegrada no prazo de 10 (dez) dias úteis, a contar da data de recebimento da notificação, sob pena de ser descontada na fatura seguinte.

10.8 A garantia será restituída após o cumprimento das obrigações contratuais, devidamente atestado pela Fiscalização e/ou Comissão da EMAP designada para esse fim.

11. REQUISITOS TÉCNICOS

11.1 Atestado(s) fornecido(s) por pessoa jurídica de direito público ou privado que comprove(m) ter o licitante executado para órgão ou entidade da administração pública direta ou indireta, federal estadual, municipal ou do Distrito Federal, ou ainda, para empresa privada, que não o próprio licitante (CNPJ diferente), o fornecimento de produto compatível com o objeto desta licitação.

12. OBRIGAÇÕES DA CONTRATADA

12.1 Executar o fornecimento rigorosamente em conformidade com todas as condições estabelecidas neste Instrumento;

12.2 Manter durante a vigência do contrato as condições de habilitação exigidas para a contratação;

12.3 Sempre que requisitada, apresentar os comprovantes de regularidade exigidos para a contratação;

12.4 Providenciar a imediata correção das falhas apontadas pela EMAP concernente a execução do contrato em um prazo máximo de 30 (trinta) dias;

12.5 Substituir, as suas expensas, os produtos entregues com vícios ou defeitos, em virtude da ação, omissão negligência, imperícia ou processos inadequados ou de qualidade inferiores em um prazo máximo de 30 (trinta) dias;

12.6 Responder pelos danos causados diretamente à EMAP ou a terceiros, decorrente de culpa ou dolo em razão do fornecimento para atendimento, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento da EMAP;

12.7 A CONTRADA deverá ser responsabilizar pelos os custos diretos e indiretos pelos os serviços que serão executados, não cabendo a EMAP qualquer custo a mais do já contratado sanar as eventuais falhas imediatamente após a sua verificação em um prazo máximo de 30 (trinta) dias;

12.8 Responder, em relação aos respectivos empregados, por todas as despesas decorrentes da execução do objeto, tais como salários, seguros de acidentes, taxas, impostos, contribuições, indenizações, distribuição de vales-refeições, vales transportes e outras exigências fiscais, sociais ou trabalhistas, devendo saldá-los na época própria, uma vez que esses empregados não manterão nenhum vínculo empregatício com a CONTRATANTE;

12.9 Responsabilizar-se pelos encargos de possível demanda judicial trabalhista, civil ou penal, relacionada à execução do contrato;

12.10 Assumir, também, a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando forem vítimas os seus empregados na execução dos serviços ou em conexão com eles, ainda que ocorridos nas dependências da EMAP;

12.11 Comunicar à EMAP, por escrito, qualquer impropriedade ou anormalidade de caráter urgente, prestando os esclarecimentos necessários, para deliberação por parte da EMAP;

12.12 Prestar à CONTRATANTE os esclarecimentos que julgar necessários para a boa execução do contrato, relatando toda e qualquer irregularidade observada em função da execução do serviço, obra ou fornecimento;

12.13 Sujeitar-se à mais ampla e irrestrita fiscalização por parte do gestor e/ou fiscal do contrato, prestando todos os esclarecimentos solicitados, de forma clara, concisa e lógica, apresentando documentação requerida e atendendo prontamente às reclamações formuladas;

12.14 Arcar com as reclamações levadas ao seu conhecimento por parte da fiscalização do contrato, cuidando imediatamente das providências necessárias para a correção, evitando repetição de fatos;

12.15 Arcar com as despesas decorrentes de qualquer infração, seja qual for, praticada pelos respectivos empregados nas instalações da CONTRATANTE;

12.16 Manter, por si, por seus prepostos e empregados, irrestrito e total sigilo sobre quaisquer dados que lhe sejam fornecidos, sobretudo quanto à estratégia de atuação da EMAP;

12.17 O contratado poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas obras, serviços ou compras, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, e, no caso particular de reforma de edifício ou de equipamento, até o limite de 50% (cinquenta por cento) para os seus acréscimos.

12.18 Manter arquivo ordenado com toda a documentação relativa à execução do contrato, a qual, quando solicitada, deverá ser encaminhada à EMAP no prazo de 48 (quarenta e oito) horas;

12.19 Abster-se de contratar empregado pertencente aos quadros de pessoal da EMAP durante a vigência do Contrato;

12.20 Informar à EMAP qualquer alteração por que passar o respectivo ato constitutivo, apresentando, no prazo de 15 (quinze) dias, contados da data do registro da modificação, cópia desta e do respectivo registro;

12.21 Substituir, caso exigido pela EMAP, independente de justificativa, qualquer empregado cuja atuação, permanência ou comportamento sejam julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina da repartição ou ao interesse do serviço público;

12.22 Receber as notificações do fiscal do contrato e da autoridade máxima da EMAP;

12.23 Abster-se de veicular publicidade acerca da presente contratação, salvo se houver prévia autorização da Administração;

12.24 Observar os prazos estabelecidos neste Instrumento.

12.25 A obrigação do contratado de manter, durante a execução do contrato, em compatibilidade com as obrigações por ele assumidas, as condições de habilitação e qualificação exigidas no curso do procedimento licitatório;

12.26 O contratado é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responderá por danos causados diretamente a terceiros ou à empresa pública ou sociedade de economia mista, independentemente da comprovação de sua culpa ou dolo na execução do contrato.

12.27 O contratado é responsável pelos encargos trabalhistas, fiscais e comerciais resultantes da execução do contrato.

12.28 Inadimplência do contratado quanto aos encargos trabalhistas, fiscais e comerciais não transfere à empresa pública ou à sociedade de economia mista a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato ou restringir a regularização e o uso das obras e edificações, inclusive perante o Registro de Imóveis.

13. OBRIGAÇÕES DA EMAP

13.1 Fiscalizar a execução/entrega dos objetos

13.2 Atestar, por meio de recibo ou simples atesto no verso da nota fiscal/fatura, a entrega do objeto;

13.3 Efetuar o pagamento no prazo pactuado, após o cumprimento das condições previamente exigidas;

13.4 Promover o acompanhamento e a fiscalização da entrega dos objetos, por servidores designado para essa atividade;

13.5 Assegurar o livre acesso dos empregados da licitante vencedora quando devidamente uniformizados e identificados, aos locais em que devam executar suas tarefas;

13.6 Efetuar o pagamento a contratada conforme pactuado, após o cumprimento das condições previamente exigidas;

13.7 Informar se as instalações e equipamentos adequados ao desenvolvimento das atividades serão de responsabilidade da contratante ou contratada.

13.8 Promover, por meio da FISCALIZAÇÃO designada neste Instrumento, o acompanhamento e a fiscalização da execução do contrato, sob os aspectos qualitativos e quantitativos, anotando em registro próprio as falhas detectadas e comunicando à CONTRATADA as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte desta última;

13.9 Permitir, quando necessário, o acesso dos empregados da CONTRATADA, devidamente identificados, às suas dependências para a fiel execução do contrato;

13.10 Prestar à CONTRATADA as informações e os esclarecimentos necessários à fiel execução contratual;

13.11 Expedir, conforme o caso, a ordem de serviço ou de fornecimento;

13.12 Efetuar o pagamento devido pelo serviço, fornecimento ou obra, desde que cumpridas todas as formalidades e exigências do contrato;

13.13 Rejeitar, no todo ou em parte, a obra, o fornecimento e/ou os serviços em desacordo com as exigências deste Contrato e do Termo de Referência;

13.14 Notificar, por escrito, a CONTRATADA quanto à ocorrência de eventual imperfeição no curso da execução do objeto, fixando prazo para a sua correção;

13.15 Fiscalizar para que, durante a vigência do Contrato, sejam mantidas as condições de habilitação exigidas na licitação;

13.16 Solicitar o reparo, a correção, a remoção, a reconstrução ou a substituição do objeto do contrato em que se verificarem vícios, defeitos ou incorreções;

13.17 Receber o objeto do contrato no dia previamente agendado, no horário de funcionamento da unidade responsável pelo recebimento;

13.18 Atestar, por meio de recibo ou de simples atesto no verso da nota fiscal/fatura, a fiel execução do contratado;

13.19 Impedir que terceiros estranhos ao contrato forneçam o objeto licitado, executem a obra ou prestem os serviços, ressalvados os casos de subcontratação admitidos no ato convocatório e no contrato;

14. CRITÉRIOS DE MEDIÇÃO

14.1 Medição

a) Para fins de emissão das notas fiscais, estes produtos serão entregues em lote único.

b) O pagamento será efetuado até em 30 dias após a emissão de nota fiscal em parcela única.

14.2 Condições:

a) O pagamento será efetuado, mediante depósito em Conta Corrente da Contratada, no Banco do Brasil S.A. ou em outra instituição bancária por ela indicada, apôs a emissão de “Cerificação da Medição” e Certificação da Nota Fiscal devidamente certificada pela Fiscalização correspondente aos produtos efetivamente entregas observadas as condições e especificações deste TR.

b) A Nota Fiscal correspondente ao fornecimento deverá ser emitida em nome da EMPRESA MARANHENSE DE ADMINISTRAÇÃO PORTUÁRIA – EMAP, CNPJ sob o nº 03.650.060/0001-48, endereço: Porto do Itaqui, s/n, Itaqui, CEP: 65.085-370, São Luís-MA, e deverá estar acompanhada de Carta de encaminhamento e com solicitação de pagamento da respectiva Nota Fiscal.

14.3 A empresa contratada deverá apresentar, para efeito de pagamento(s), juntamente com a(s) nota(s) fiscal(is):

- Carta endereçada à EMAP formalizando o pedido de pagamento;
- Certidão negativa de débitos relativos a créditos tributários federais e a divida ativa da união
- Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS);
- Certidão Negativa de Débitos Trabalhistas (CNDT);
- Certidão Negativa de Débitos Estadual e Municipal (CND).

14.4 O pagamento dos fornecimentos realizados pela empresa contratada estará condicionado, também, à comprovação de regularidade da empresa contratada junto ao Cadastro Estadual de Inadimplentes – CEI, do Estado do Maranhão, conforme estabelecido no Decreto Nº 21.331, de 20 de julho de 2005;

14.5 Nenhum pagamento será efetuado à empresa contratada enquanto estiver pendente liquidação de qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência contratual;

15. CRITÉRIOS

15.1O critério de julgamento da licitação será o menor preço.

15.2Os itens deste TR são considerados comuns.

15.3Regime de execução: empreitada por preço global

15.4A licitação ocorrerá pelo modo de disputa aberto, a partir de lances públicos, sucessivos e decrescentes, a fim de que alcance a proposta mais vantajosa para a empresa.

15.5Ressalta-se que o orçamento para a presente contratação ocorreu de forma sigilosa

16. VISITA TÉCNICA

Não necessita de visita técnica.

PREGÃO ELETRÔNICO N° 021/2024 – EMAP
ANEXO II

MODELO DE PROPOSTA DE PREÇOS

Prezados Senhores,

Pela presente, submetemos à apreciação de V.Sa., a nossa proposta de preço relativa a licitação **PREGÃO ELETRÔNICO N° 021/2024 – EMAP**, assumindo inteira responsabilidade por quaisquer erros ou omissões que venham a ser verificados na preparação da mesma, bem como concordamos com a totalidade das instruções e critérios de qualificação definidos no Edital, e declaramos, ainda, que temos pleno conhecimento das condições em que se desenvolverão os serviços, *e que atendemos plenamente às exigências de habilitação*, comprometendo-se a observar a legislação trabalhista, previdenciária e de saúde e medicina no trabalho, responsabilizando-se pela formalização e registro contratuais e pela previsão de gastos com meio ambiente do trabalho, incluindo equipamentos de proteção.

RAZÃO SOCIAL:
ENDEREÇO:
CNPJ:
DADOS BANCÁRIOS:

ITEM	DESCRIÇÃO	UNID.	QTDE.	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	Solução de Next Generation Firewall em Alta Disponibilidade com garantia e suporte por 36 meses		2		
2	Solução de Gerenciamento Centralizado com garantia e suporte por 36 meses		1		
3	Solução de detecção e resposta estendidas para estações de trabalho e servidores com garantia e suporte por 36 meses		700		
4	Solução de Zero Trust Network Access (ZTNA) com capacidade para suportar 200 usuários com garantia e suporte por 36 meses		1		
5	Serviço de instalação, configuração e migração da solução		1		
VALOR TOTAL GLOBAL (R$)					

Observação: Deve-se considerar as informações constantes do Termo de Referência (Anexo I) para formulação das propostas de preços.

PREÇO TOTAL GLOBAL: R$ _____,___ (_____).

PRAZO DE VALIDADE DA PROPOSTA: ____ (_____) dias.

PRAZO DE EXECUÇÃO: até 12 (doze) meses.

Data, ____de _____de 2024.

_____
Assinatura do responsável legal da licitante

PREGÃO ELETRÔNICO N° 021/2024 – EMAP

ANEXO III

MODELO DE TERMO DE COMPROMISSO DE CUMPRIMENTO DA LEGISLAÇÃO TRABALHISTA, PREVIDENCIÁRIA E DE SAÚDE E MEDICINA DO TRABALHO

Ref.: **PREGÃO ELETRÔNICO N° 021/2024 – EMAP**

A empresa _____, inscrita no CNPJ nº_____, com sede na _____, por intermédio de seu representante legal o (a) Sr(a) _____, R.G. nº_____, CPF nº _____, DECLARA para os fins de direito, caso seja declarada vencedora do **PREGÃO ELETRÔNICO N° 021/2024 – EMAP** e celebrado o respectivo Contrato Administrativo, que se compromete a observar a legislação trabalhista, previdenciária e de saúde e medicina no trabalho, responsabilizando-se pela formalização e registro contratuais e pela previsão de gastos com meio ambiente do trabalho, incluindo equipamentos de proteção.

São Luís, __ de _____ de 2024.

_____
Assinatura do responsável legal da licitante

PREGÃO ELETRÔNICO N° 021/2024 – EMAP

ANEXO IV

DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

Ref.: **PREGÃO ELETRÔNICO N° 021/2024 – EMAP**

DECLARO, sob as penas da Lei, que cumpro os requisitos estabelecidos no Art. 3º da Lei Complementar nº 123, de 14 de dezembro de 2006, alterada pela Lei nº 11.488, de 15 de junho de 2007, em seu Art. 34, que a Empresa _____ (denominação da pessoa jurídica), CNPJ nº. _____ está apta a usufruir do tratamento favorecido estabelecido nos artigos 42 ao 49 da referida Lei Complementar.

São Luís, __ de _____ de 2024.

_____

Assinatura do responsável legal da licitante

PREGÃO ELETRÔNICO N° 021/2024 – EMAP

ANEXO V

DECLARAÇÃO DAS CONDIÇÕES DE EMPREGABILIDADE DE MENOR

A Empresa _____, inscrita no CNPJ/MF sob o nº _____, por intermédio de seu representante legal o Sr.(a) _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, D E C L A R A, sob as penas da lei, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

São Luís, __ de _____ de 2024.

_____
Assinatura do responsável legal da licitante

PREGÃO ELETRÔNICO N° 021/2024 – EMAP

ANEXO VI

QUESTIONÁRIO PARA REALIZAÇÃO DE DILIGÊNCIAS APROPRIADAS

1. PERFIL DA EMPRESA

1.1 **Qual a sua razão social?**

_____

1.2 **Quantos empregados sua empresa possui?**

_____

2. Histórico

2.1 Algum integrante da Alta Administração da sua empresa já foi responsabilizado em razão de fraude, corrupção ou improbidade administrativa nos últimos 05 anos?

( ) SIM ( ) NÃO

2.2 A sua empresa, alguma controladora, controlada, coligada ou consorciada, esteve submetida à investigação ou avaliação externa relacionada a fraude, corrupção ou improbidade administrativa por algum órgão ou agência (CGU, CVM, etc.) nos últimos 5 anos?

( ) SIM ( ) NÃO

3. Programa de Integridade

3.1 A sua empresa possui Código de Conduta, Código de Ética ou documento correlato que descreva condutas éticas que devem ser observadas pelos integrantes da Alta Administração, empregados próprios e/ou terceirizados?

( ) SIM ( ) NÃO

3.2 A sua empresa possui um programa ou uma política de integridade estruturado com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos, incluindo a prática de lavagem de dinheiro?

( ) SIM ( ) NÃO

3.3 A sua empresa possui uma política de patrocínio ou documento correlato que disponham sobre a

concessão de apoio ou contribuição financeira a eventos, feiras, seminários, programas sociais, através de entidades não governamentais, e demais iniciativas?

( ) SIM ( ) NÃO

3.4 A sua empresa possui uma política ou instrumento correlato que estipule padrões de conduta e práticas de gestão no relacionamento com terceiros/stakeholders?

( ) SIM ( ) NÃO

3.5 A sua empresa promove treinamentos periódicos destinados à Alta Administração, a empregados próprios e/ou terceiros sobre suas normativas internas, políticas anticorrupção e de prevenção a riscos de compliance, código de conduta e demais documentos correlatos?

( ) SIM ( ) NÃO

3.6 A sua empresa possui procedimento ou instrumento de efetivação de diligências prévias de verificação de conformidade, aplicáveis às partes relacionadas/ stakeholders (fornecedores, clientes, parceiros, etc.)?

( ) SIM ( ) NÃO

3.7 A sua empresa disponibiliza canal de denúncias de irregularidades, com ampla divulgação e de fácil acesso a todos os empregados próprios, terceirizados e para a sociedade em geral?

( ) SIM ( ) NÃO

3.8 A sua empresa possui política ou previsões normativas a respeito da proteção àquele pretenda denunciar violação ao Programa de Integridade e/ou demais normas?

( ) SIM ( ) NÃO

3.9 A sua empresa possui mecanismos de investigação a indícios cometimento de atos que envolvam riscos de compliance, tais como canais de denúncias?

( ) SIM ( ) NÃO

3.10 Há, em sua empresa, estrutura/setor/órgão/departamento/unidade específica, autônoma e independente que realize mapeamento e gestão de riscos de compliance, além de investigações, quando necessário, decorrentes de denúncias?

( ) SIM ( ) NÃO

Solicitamos que, caso existam normas, códigos e políticas de integridade ou derivadas, que seja remetida cópia à EMAP juntamente com este questionário, ou indicado, no espaço abaixo, o endereço eletrônico em que podem ser acessadas.

4. Relacionamento com Terceiros

4.1 A sua empresa possui um guia, manual ou documento correlato de clientes e fornecedores que oriente todos aqueles que mantenham contrato com a sua empresa à adoção de uma postura ética com absoluta integridade e decoro no desenvolvimento de suas atividades?

( ) SIM ( ) NÃO

4.2 Há previsão, nos contratos firmados por sua empresa com terceiros (fornecedores, clientes ou parceiros), de cláusulas que determinem a manutenção da conformidade com as leis anticorrupção aplicáveis e vigentes?

( ) SIM ( ) NÃO

Há previsão, nos contratos firmados por sua empresa com terceiros (fornecedores, clientes ou parceiros), de cláusulas que determinem a aplicação do seu Programa de Integridade, Código de Conduta ou documentos correlatos?

( ) SIM ( ) NÃO

5 Declarações

5.1 Declaração de Não-Relacionamento com Agentes Públicos

Declaro, para fins de compromisso com a integridade corporativa, que:

Algum integrante da Alta Administração ou seus familiares em linha reta ou colateral até o segundo grau, ocupa cargo eletivo ou de confiança na Administração Pública direta, indireta, autárquica, fundacional ou em estatais da União, Estados, Distrito Federal ou Municípios.

( ) SIM ( ) NÃO

Em caso de resposta positiva, indique a pessoa e o cargo.

Algum integrante da Alta Administração da sua empresa é familiar, seja em linha reta ou colateral até o segundo grau, de empregado da EMAP ou de membro de Conselhos Vinculados?

( ) SIM ( ) NÃO

Em caso de resposta positiva, indique a pessoa e o cargo.

5.2 Declaração de Veracidade

Declaro que todas as informações prestadas neste Questionário, bem como os documentos nele inseridos como anexos, são verdadeiras, completas e atualizadas.

São Luís/MA,_____de_____de 2024.

Nome por extenso:	
Cargo Ocupado na Empresa	
CPF	
Matrícula (se houver)	

PREGÃO ELETRÔNICO N° 021/2024 – EMAP

ANEXO VII

MINUTA DO CONTRATO

CONTRATO Nº NNN/202N/00-EMAP

CONTRATO QUE ENTRE SI CELEBRAM A EMPRESA MARANHENSE DE ADMINISTRAÇÃO PORTUÁRIA E [RAZÃO SOCIAL] PARA O FORNECIMENTO DE EVOLUÇÃO TECNOLÓGICA DE PROTEÇÃO DE BORDA, ESTAÇÕES DE TRABALHO E SERVIDORES DA EMAP - EMPRESA MARANHENSE DE ADMINISTRAÇÃO PORTUÁRIA, BEM COMO SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO.

CONTRATANTE: A **EMPRESA MARANHENSE DE ADMINISTRAÇÃO PORTUÁRIA**, empresa pública, com capital social totalmente subscrito e integralizado pelo Estado do Maranhão, personalidade jurídica de direito privado, autonomia administrativa, técnica, patrimonial e financeira, inscrita no Cadastro Nacional da Pessoa Jurídica sob o nº 03.650.060/0001-48, criada pela Lei Estadual nº 7.225, de 31 de agosto de 1998, vinculada à Secretaria de Estado de Desenvolvimento Econômico e Programas Estratégicos – SEDEPE, com sede no Porto do Itaqui, s/n, Itaqui, São Luís, Maranhão, daqui por diante denominada EMAP, representada por [seu/sua] [cargo/função], [o/a Sr/a. Nome Completo], portador da Cédula de Identidade nº [Número] [Órgão Expedidor], inscrito no Cadastro de Pessoas Físicas sob o nº [Número], e por [seu/sua] [cargo/função], [o/a Sr/a. Nome Completo], portadora da Cédula de Identidade nº [Número] [Órgão Expedidor], inscrita no Cadastro de Pessoas Físicas sob o n° [Número] e, de outro lado;

CONTRATADO: [o/a] [Razão Social], inscrito no Cadastro Nacional da Pessoa Jurídica sob o nº [Número], estabelecido no(a) [Endereço Completo], [Cidade] (UF), CEP [Número], representado por [seu/sua] [cargo/função], [o/a Sr/a. Nome Completo], portador da Cédula de Identidade nº [Número] [Órgão Expedidor], inscrito no Cadastro de Pessoas Físicas sob o nº [Número], na forma da representação legal que lhe é outorgada por meio de [procuração/contrato social/estatuto social];

Os **CONTRATANTES**, em consonância com a Lei nº 13.303/2016 e com o Regulamento de Licitações e Contratos da Empresa Maranhense de Administração Portuária, e tendo em vista o constante do processo administrativo nº 1381/2024, têm entre si justo e avençado o presente

Inicial + Matrícula de quem elaborou

contrato, decorrente do(a) Pregão Eletrônico N° 021/2024 – EMAP, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1 O presente contrato tem como objeto o fornecimento de evolução tecnológica de proteção de borda, estações de trabalho e servidores da EMAP - Empresa Maranhense De Administração Portuária, bem como serviço de instalação e configuração, conforme especificações e quantitativos estabelecidos no Edital do Pregão identificado no preâmbulo (e respectivos anexos, em especial o Anexo I – Termo de Referência) e na proposta vencedora, os quais integram este instrumento, independente de transcrição.

CLÁUSULA SEGUNDA – DOS PRAZOS DE EXECUÇÃO E DE FORNECIMENTO

2.1 A contratada terá o prazo de até 60 (Sessenta) dias corridos, a partir da data indicada na Ordem de Fornecimento, para concluir a entrega dos equipamentos.
2.2 O prazo de execução contratual será de 12 (doze) meses, contando-se a partir da data indicada na Ordem de Fornecimento, a ser emitida pela EMAP.
2.3. O fornecimento deve acontecer de forma unitária.

CLÁUSULA TERCEIRA – DO PREÇO

3.1 O valor total deste contrato é R$ [Número] (Numeral Por Extenso).
3.2 No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.
3.3. Os preços são fixos e irreajustáveis no prazo de um ano contado da data de apresentação das propostas.

CLÁUSULA QUARTA – DO PAGAMENTO

4.1 O(s) pagamento(s) será(ão) efetuado(s) após a entrega dos produtos, em lote único, em até 30 (trinta) dias após a apresentação da fatura, por meio de depósito em conta corrente da empresa contratada, em instituição bancária por ela indicada, mediante apresentação da nota fiscal, ou fatura/boleto com código de barras, correspondente serviços/produtos executados ou fornecidos, e certificado pelo fiscal do contrato, observadas as condições propostas e aceitas pela EMAP.
4.1.1 A nota(s) fiscal(ais) deverá(ão) ser emitida até o dia 20 (vinte) do mês subsequente à conclusão dos serviços e fornecimentos, em nome da EMPRESA MARANHENSE DE ADMINISTRAÇÃO PORTUÁRIA – EMAP, CNPJ sob o nº 03.650.060/0001-48, endereço: Porto do Itaqui, s/n, Itaqui, CEP: 65.085-370, São Luís – MA.
4.1.2 O pagamento se dará por meio do Banco [Descrever], Agência [Número] e Conta [Número].
4.1.3 Cumpre ao Contratado comunicar, por escrito, à Contratante a instituição bancária e os números da agência, da conta e da operação na hipótese de modificação dos dados constantes na cláusula anterior.
4.2 O pagamento somente será autorizado depois de efetuado o “atesto”, pelo empregado competente, na nota fiscal apresentada.

4.3.O contratado deverá solicitar, formalmente, o pagamento à contratante, apresentando o pedido de pagamento, devidamente instruído, ao Protocolo da Empresa Maranhense de Administração Portuária.

4.4 Havendo erro na apresentação da nota fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que o Contratado providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

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

4.6 Antes de cada pagamento ao Contratado, será realizada consulta para verificar a manutenção das condições de habilitação exigidas no edital.

4.6.1 O pagamento também estará condicionado à inexistência de pendências do Contratado no Cadastro Estadual de Inadimplentes do Estado do Maranhão – CEI, nos termos da Lei Estadual nº 6.690, de 11 de julho de 1996 (regulamentado pelo Decreto n.º 21.331, de 20 de julho de 2005).

4.7 Constatando-se a situação de irregularidade do Contratado, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério exclusivo da Contratante.

4.8 Persistindo a irregularidade, a Fiscalização comunicará o fato à Gerência Jurídica da Contratante, a fim de que, assegurados ao Contratado a ampla defesa e o contraditório, sejam adotadas as medidas jurídicas cabíveis.

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

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

4.10 Nos casos de eventuais atrasos de pagamento, desde que o Contratado não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX) I = (6 / 100)

I = 0,00016438

TX = Percentual da taxa anual = 6%

CLÁUSULA QUINTA – DAS ALTERAÇÕES CONTRATUAIS

5.1 É vedado todo e qualquer ajuste que resulte em violação da obrigação de licitar.
5.2 Eventuais alterações contratuais reger-se-ão pela disciplina dos artigos 72 e 81 da Lei nº 13.303/2016, realizando-se mediante a celebração de termo de aditamento.
5.3 O contrato somente poderá ser alterado por acordo entre as partes.
5.4 O Contratado poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem na compra, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.
5.5 Nenhum acréscimo ou supressão poderá exceder o limite estabelecido no item anterior, salvo as supressões resultantes de acordo celebrado entre os contratantes.
5.6 A criação, a alteração ou a extinção de quaisquer tributos ou encargos legais, bem como a superveniência de disposições legais, quando ocorridas após a data da apresentação da proposta, com comprovada repercussão nos preços contratados, implicarão a revisão destes para mais ou para menos, conforme o caso.
5.7 A variação do valor contratual para fazer face ao reajuste de preços previsto no próprio contrato e as atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento nele previstas, bem como o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido, não caracterizam alteração do contrato e podem ser registrados por simples apostila, dispensada a celebração de aditamento.

CLÁUSULA SEXTA – DO RECEBIMENTO DO OBJETO
6.1 As condições e os prazos de recebimento do objeto são aqueles previstos no Termo de Referência.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATANTE
7.1 São obrigações da Contratante, além daquelas previstas no item 13 do Termo de Referência (Anexo I do Edital):
7.1.1 No que diz respeito ao objeto, observar os prazos e as condições estabelecidas no Edital e respectivos anexos;
8.1.2 verificar minuciosamente, no prazo fixado, a conformidade do objeto com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento da prestação do serviço;
7.1.3 comunicar ao Contratado, por escrito, sobre imperfeições, falhas ou irregularidades Verificadas na execução do objeto;
7.1.4 acompanhar e fiscalizar o cumprimento das obrigações do Contratado, por meio de comissão ou de empregado especialmente designado;
7.1.5 efetuar o pagamento ao Contratado no valor correspondente ao efetivo fornecimento do objeto, no prazo e na forma estabelecidos no Edital e respectivos anexos.
7.2 A Contratante não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DO CONTRATADO

8.1 Além das obrigações constantes no item 12 do Termo de Referência (Anexo I do Edital), o Contratado deve cumprir todas as obrigações constantes no Edital, seus anexos, além da sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, bem como:

8.1.1 responder perante a Contratante e terceiros pela cobertura dos riscos e acidente de trabalho dos seus empregados, prepostos ou contratados, bem como por todos os ônus, encargos, perdas e danos, porventura resultantes da execução dos serviços para completa execução deste contrato;

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

8.1.3 manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

8.1.4 indicar preposto para representá-la durante a execução do contrato;

8.1.5 reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, e responder por danos causados diretamente a terceiros ou à Contratante, independentemente da comprovação de sua culpa ou dolo na execução do contrato;

8.1.6 responder pelos encargos trabalhistas, fiscais e comerciais resultantes da execução do contrato;

8.1.7 observar as normas de segurança, saúde e meio ambiente da Contratante, em consonância com o disposto no Termo de Referência;

8.2 É vedado ao contratado caucionar ou utilizar este Contrato para qualquer operação financeira.

8.3 O Contratado declara conhecer e compromete-se a observar e a fazer os respectivos empregados e dirigentes respeitarem o Código de Conduta (disponível em: http://www.emap.ma.gov.br/_files/arquivos/codigo-de-conduta-emap.pdf), a Política de Transações com Partes Relacionadas (disponível em: http://www.emap.ma.gov.br/_files/arquivos/Politica-de-Transacoes-com-Partes-Relacionadas.pdf), o Guia de Clientes e Fornecedores (disponível em: http://www.emap.ma.gov.br/_files/arquivos/Guia_de_Clientes_e_Fornecedores_EMAP.pdf), a Política de Integridade (disponível em: http://www.emap.ma.gov.br/_files/arquivos/POLITICA_DE_INTEGRIDADE.pdf), a Política de Segurança da Informação, suas Políticas Técnicas e procedimentos (disponível em: http://www.emap.ma.gov.br/emap/gestao/seguranca-da-informacao/) e as Regras de Ouro do Trânsito (disponível em: http://www.emap.ma.gov.br/emap/gestao/seguranca-do-trabalho), todos documentos da Empresa Maranhense de Administração Portuária.

8.4. Prestar os esclarecimentos necessários para a boa execução do contrato, relatando toda e qualquer irregularidade observada em função da execução do contrato;

8.5. Responsabilizar-se pelas por todas as despesas decorrentes da execução dos serviços contratados;

8.6 A contratada deverá assegurar que o acesso e tratamento de dados pessoais dos representantes da contratante (EMAP) se dará exclusivamente para a execução do contrato,

devendo resguardá-los de acessos indevidos e incidentes e, ao final da vigência do contrato, deverá providenciar a eliminação destes de sua base de dados
8.7. Atender todas as condições e prazos previstos no Termo de Referência e demais anexos.

CLÁUSULA NONA – DAS SANÇÕES ADMINISTRATIVAS
9.1 O Contratado cometerá infração administrativa se:
9.1.1 apresentar documentação falsa;
9.1.2 retardar a execução do objeto;
9.1.3 falhar na execução contratual;
9.1.4 fraudar na execução contratual;
9.1.5 comportar-se de modo inidôneo;
9.1.6 não mantiver a proposta;
9.1.7 inexecutar, total ou parcialmente, qualquer das obrigações assumidas em decorrência da contratação;
9.1.8 fizer declaração falsa.
9.2 Observada a ampla defesa, o Contratado que cometer qualquer das infrações discriminadas acima ficará sujeito, sem prejuízo da responsabilidade civil e criminal e da rescisão unilateral do contrato, às seguintes sanções:
9.2.1 advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;
9.2.2 multa moratória, pelo atraso injustificado na execução contratual, configurado mediante o retardamento dessa execução, ou a falha na execução contratual, ou, ainda, a inexecução, total ou parcial, de qualquer das obrigações assumidas em decorrência da contratação;
9.2.3 multa compensatória, pela apresentação de documentação falsa, pela falha na execução contratual, pela fraude na execução contratual, pelo comportamento de modo inidôneo, pela não manutenção da proposta, pela inexecução, total ou parcial, de obrigação assumida em decorrência da contratação e pela prestação de declaração falsa;
9.2.4 suspensão temporária de participação em licitação e impedimento de contratar com a Contratante, por prazo não superior a 2 (dois) anos.
9.3 As sanções previstas nos itens 9.2.1 e 9.2.4 poderão ser aplicadas juntamente com a multa compensatória prevista no item 9.2.3, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis.
9.3.1 A multa a que alude o item 9.2.2 não impede que a Contratante rescinda o contrato e aplique as outras sanções previstas nesta Lei.
9.3.1.1 A multa a que alude o item 9.2.2, aplicada após regular processo administrativo, será descontada da garantia do respectivo contratado, se houver.
9.3.1.2 Se a multa moratória for de valor superior ao valor da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Contratante ou, ainda, quando for o caso, cobrada judicialmente.
9.4 Para fins do disposto no item 9.1.5, reputar-se-ão inidôneos atos tais como os descritos nos artigos 337-F, 337-L e 337-M, §2º do Código Penal.
9.5 Para fins do disposto no item 9.2.2, a CONTRATADA fica sujeita à multa moratória equivalente a 1% (um por cento) do valor unitário do bem em atraso, por dia, por unidade, até o limite de 20% (vinte por cento) do valor do contrato.

9.5.1 Considera-se inexecução parcial o atraso injustificado no prazo de entrega até o limite de 10 (dez) dias.
9.6 Para fins do disposto no item 9.2.3, a CONTRATADA fica sujeita à multa de, no máximo, 30% (trinta por cento) do valor do contrato.
9.6.1 Considera-se inexecução total o atraso injustificado no prazo de entrega superior a 10 (dez) dias.
9.6.2 Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem 9.6, será aplicada de forma proporcional à obrigação inadimplida.
9.7 O não-cumprimento de obrigação contratual acessória, a exemplo de eventual garantia exigida para os produtos, sujeitará o Contratado à multa de até 10% (dez por cento) do valor do contrato.
9.8 O valor da multa poderá ser descontado das faturas devidas ao Contratado.
9.8.1 O valor da multa também poderá ser descontado da garantia de execução contratual, se houver.
9.8.2 Se os valores das faturas ou da garantia de execução contratual forem insuficientes, fica o Contratado obrigado a recolher a importância devida no prazo de 15 (quinze) dias, contados da comunicação oficial.
9.8.3 Esgotados os meios administrativos para a cobrança do valor devido pelo Contratado à Contratante, o débito será cobrado judicialmente.
9.9 O contratado sujeita-se à suspensão temporária de participação em licitação e ao impedimento de contratar com a Contratante:
9.9.1 pelo prazo de 2 (dois) anos, quando apresentar documentação falsa, fraudar a execução contratual, comportar-se de modo inidôneo ou fizer declaração falsa;
9.9.2 por prazo não superior a 2 (dois) anos, quando retardar a execução do objeto, falhar na execução do objeto, inexecutar o objeto contratual ou não mantiver a proposta.
9.10 A sanção prevista no item 9.9.1 poderá ser aplicada às empresas ou aos profissionais que, em razão deste contrato:
9.10.1 tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
9.10.2 tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
9.10.3 demonstrem não possuir idoneidade para contratar com a Empresa Maranhense de Administração Portuária em virtude de atos ilícitos praticados.

CLÁUSULA DÉCIMA– DA RESCISÃO

10.1 Constituem motivos, entre outros, para a rescisão contratual:
10.1.1 o não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;
10.1.2 o cumprimento irregular de cláusulas contratuais, especificações, projetos ou prazos;
10.1.3 a lentidão do seu cumprimento, levando a Empresa Maranhense de Administração Portuária a comprovar a impossibilidade do fornecimento nos prazos estipulados;
10.1.4 o atraso injustificado no início da obra, serviço ou fornecimento;
10.1.5 a paralisação do fornecimento, sem justa causa e prévia comunicação à Empresa Maranhense de Administração Portuária;

10.1.6 a subcontratação total ou parcial do seu objeto, a associação do contratado com outrem, a cessão ou a transferência, total ou parcial, bem como a fusão, cisão ou incorporação não admitidas no edital, termo de referência ou neste contrato;
10.1.7 o desatendimento das determinações regulares da Empresa Maranhense de Administração Portuária decorrentes do acompanhamento e fiscalização do contrato;
10.1.8 a decretação de falência ou a instauração da insolvência civil;
10.1.9 a dissolução da sociedade ou o falecimento do contratado;
10.1.10 a alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato;
10.1.11 a ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato.
10.2 Os casos de rescisão contratual serão formalmente motivados, assegurando-se ao Contratado o direito à prévia e ampla defesa.

CLÁUSULA DÉCIMA PRIMEIRA – DA FISCALIZAÇÃO

11.1 O objeto deste Contrato será fiscalizado pelo(a) Sr(a). xxxx daqui por diante denominada simplesmente "Fiscalização", independentemente de qualquer outra supervisão, assessoramento e/ou acompanhamento dos serviços, que venham a ser determinados pela EMAP, a seu exclusivo juízo, podendo ser substituído pelo(a) Sr(a). xxxxxxx, em seu impedimento, conforme item 9 do Termo de Referência (Anexo I do Edital).
11.2. Caberá à Fiscalização:
11.2.1. Transmitir à CONTRATADA as determinações que julgar necessárias, nos termos do princípio da legalidade;
11.2.2. Receber formalmente da Gerência de Compras e Contratos – GECOC o processo e o contrato, mediante a assinatura do Termo de Recebimento, para a devida fiscalização e gestão da execução do objeto contratado, analisando pormenorizadamente as Cláusulas Contratuais;
11.2.3. Os gestores designados anotarão em registro próprio todas as ocorrências, determinando o que for necessário à regularização das faltas ou defeitos observados;
11.2.4. Observar o prazo contratual de modo evitar descontinuidades destes serviços considerados de natureza contínua;
11.2.5. Recusar os serviços que não tenham sido realizados de acordo com as condições ajustadas;
11.2.6. Ordenar a imediata retirada de suas dependências, de empregados da CONTRATADA, cuja permanência seja inconveniente, ou que venha embaraçar ou dificultar a ação fiscalizadora, correndo por exclusiva conta da CONTRATADA quaisquer ônus decorrentes das leis trabalhistas e previdenciárias, bem como qualquer outra que tal fato imponha;
11.2.7. Acusar a falta de atendimento às solicitações por parte da Contratada, bem como o atendimento inadequado, incompleto e/ou retardatário, notificando-a para que proceda à imediata regularização, sob pena de serem aplicadas as sanções e penalidades previstas neste instrumento e na lei;
11.2.8. A ação ou omissão total ou parcial da Fiscalização da EMAP não eximirá à CONTRATADA da responsabilidade por eventuais vícios da execução dos serviços, objeto da contratação;

11.2.9. A identificação dos responsáveis pela solicitação, pela avaliação da qualidade e pelo ateste dos serviços;
11.2.10. Informar à administração sobre eventuais vícios, irregularidades ou baixa qualidade dos serviços prestados pela contratada, bem como propor soluções que entender cabíveis para regularização das faltas e defeitos observados, comunicando, quando cabível, alterações do quantitativo do objeto ou modificação da forma de execução;
11.2.11. Além da lista acima, por não exaustiva, caberá ao fiscal tomar todas as providências atinentes aos princípios da administração pública, cuja finalidade última será a consecução do interesse público, fazendo cumprir, no que couber, as Obrigações da Contratada e da Contratante.

CLÁUSULA DÉCIMA SEGUNDA – DA FONTE DE RECURSOS
12.1. As despesas decorrentes dos serviços, objeto desta contratação, correrão por conta da disponibilidade financeira e orçamentária no Orçamento Geral da EMAP, fonte 227 – recursos das empresas estatais – exercício financeiro – 2024 – CAPEX TI - Aquisição de 2 aplliances de Firewall e XDR.

CLÁUSULA DÉCIMA TERCEIRA – CLÁUSULA ANTICORRUPÇÃO
13.1 Em demonstração de comprometimento e responsabilidade, as Partes declaram conhecer e concordar integralmente com o estabelecido na Lei nº 12.846/2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, e se comprometem a observar e a fazer observar, inclusive por seus subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de contratação e de execução do objeto contratual. Sendo assim, na execução do presente Contrato, é vedado à Empresa Maranhense de Administração Portuária e ao Contratado e/ou a empregado, preposto e/ou gestor seu:
13.1.1 ao longo da vigência deste ajuste e após, prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada, ou a quem quer que seja;
13.1.2 comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos na Lei nº 12.846/2013;
13.1.3 criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o presente Contrato;
13.1.4 obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações do presente Contrato, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais;
13.1.5 manipular ou fraudar o equilíbrio econômico-financeiro do presente Contrato;
13.1.6 dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional; e/ou,
13.1.7 de qualquer maneira fraudar o presente Contrato, assim como realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº 12.846/2013 (conforme alterada), do Decreto nº 8.420/2015 (conforme alterado) ou de quaisquer outras leis

ou regulamentos aplicáveis ("Leis Anticorrupção"), ainda que não relacionadas com o presente Contrato.
13.2 Constatada administrativamente qualquer prática contrária aos deveres estipulados nesta cláusula, a Parte poderá notificar a outra e exigir que essa Parte tome as medidas corretivas necessárias em um prazo razoável.
13.3 Se a Parte notificada falhar ao tomar as medidas corretivas necessárias, ou se essas medidas não forem possíveis, poderá invocar defesa, provando que, quando as evidências da violação surgiram, tinha colocado em prática medidas preventivas anticorrupção, capazes de detectar o ato de corrupção e promover uma cultura de integridade na organização.
13.4 Se nenhuma medida corretiva for tomada, a Parte notificante poderá, a seu critério, independentemente das sanções aplicáveis à conduta, proceder à imediata rescisão deste Contrato, sem prejuízo da aplicação das penalidades devidas.

CLÁUSULA DÉCIMA QUARTA – DA VIGÊNCIA CONTRATUAL
14.1 O prazo de vigência do Contrato de que trata esta licitação será de 15 (quinze) meses, a contar da data de sua assinatura.

CLÁUSULA DÉCIMA QUINTA – DA GARANTIA DE EXECUÇÃO CONTRATUAL
15.1 A Contratada prestará garantia, em até 10 (dez) dias corridos após a assinatura do contrato, no percentual 5% (cinco por cento) do valor global contratado, observado as indicações do Projeto Básico/Termo de Referência e deste Edital, com validade para todo o período contratual, devendo ser renovada a cada prorrogação, em uma das modalidades a seguir, não sendo concedido, em nenhuma hipótese, prazo para apresentação da garantia após esse prazo:
15.1.1 caução em dinheiro;
15.1.2 seguro-garantia;
15.1.3 fiança bancária.
15.2 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:
15.2.1 prejuízos advindos do não cumprimento do contrato;
15.2.2 multas aplicadas à Contratada;
15.2.3 prejuízos diretos causados à Contratante decorrentes de culpa ou de dolo durante a execução do contrato;
15.2.4 obrigações previdenciárias e trabalhistas não honradas pela Contratada.
15.3 Se a opção de garantia for a caução em dinheiro, a Contratada deverá solicitar informações à EMAP referentes ao nome da instituição financeira, aos números da conta corrente e da agência bancária, e ao código identificador, para efeito de depósito do crédito, sendo que o valor caucionado será restituído considerando-se os critérios vigentes de remuneração da poupança aplicados à época da devolução.
15.4 Se a opção recair em seguro-garantia, deverá ser feita a entrega da apólice em original, acompanhada de comprovante de pagamento do respectivo prêmio, devendo ainda conter expressamente cláusula de atualização financeira, de imprescritibilidade, inalienabilidade e de irrevogabilidade e deverá ser válida por pelo menos 90 (noventa) dias consecutivos após o prazo de validade deste contrato. A modalidade seguro garantia somente será aceita se contemplar todos os eventos indicados no parágrafo primeiro da cláusula décima deste Contrato.

15.5 Se a opção recair em fiança bancária, deverá ser feita a entrega da Carta de Fiança, em original, assinada pelo(s) representante(s) legal(is) do emitente devidamente comprovado, devendo conter expressamente cláusula de atualização financeira, de imprescritibilidade, inalienabilidade e de irrevogabilidade e deverá ser válida por pelo menos 90 (noventa) dias consecutivos após o prazo de validade do contrato.
15.6 Caso ocorra a prorrogação do Contrato, a Contratada fica obrigada a apresentar, no ato da assinatura do Termo Aditivo ou em até 10 (dez) dias úteis dessa data, a critério da EMAP, a renovação da caução prestada quando a mesma tiver sido feita nas modalidades de seguro garantia ou fiança bancária.
15.7 A Contratante poderá descontar do valor da garantia toda e qualquer importância que lhe for devida, a qualquer título, pela Contratada, inclusive multas.
15.8 Se o desconto se efetivar no decorrer do prazo contratual, a caução deverá ser reintegrada no prazo de 10 (dez) dias úteis, a contar da data de recebimento da notificação, sob pena de ser descontada na fatura seguinte.
15.9 A garantia será restituída após o cumprimento das obrigações contratuais, devidamente atestado pela Fiscalização e/ou Comissão da EMAP designada para esse fim.

CLÁUSULA DÉCIMA SEXTA – DO PROGRAMA DE INTEGRIDADE

16.1. Para os fins desta Cláusula, aplicam-se as disposições constantes da Lei Ordinária nº 11.463, de 04 de maio de 2021, que estabelece a exigência de programa de integridade às empresas que celebrarem contrato, consórcio, convênio, concessão ou parceria público-privada com a Empresa Maranhense de Administração Portuária-EMAP, nos casos de enquadramento e nos limites anuais previstos na referida lei.
16.2. O Programa de Integridade exigido por essa Lei consiste no conjunto de mecanismos e procedimentos de integridade, controle e auditoria realizado no âmbito das empresas privadas, objetivando genericamente prevenir, detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública do Estado do Maranhão, bem como:
I - proteger a administração pública estadual dos atos lesivos que resultem em prejuízos materiais ou financeiros causados por irregularidades, desvios de ética e de conduta e fraudes contratuais;
II - garantir a execução dos contratos e demais instrumentos em conformidade com a lei e regulamentos pertinentes a cada atividade contratada;
III - reduzir os riscos inerentes aos contratos e demais instrumentos, provendo maior segurança e transparência;
IV - obter melhores desempenhos e garantir a qualidade nas relações contratuais em sua consecução.
16.3. No ato da assinatura do contrato, a Contratada deverá comprovar a existência de Programa de Integridade, que será avaliado de acordo com os parâmetros constantes no art. 5º da Lei Ordinária nº 11.463, de 04 de maio de 2021, devendo apresentar relatório de perfil e relatório de conformidade do Programa, conforme art. 6º da referida lei.
16.4. Na hipótese de inexistência de Programa de Integridade implantado no âmbito da empresa, a Contratada deverá implantar o Programa no prazo de 120 (cento e vinte) dias corridos, a partir da data de celebração do contrato.

16.5. Os custos e despesas com a implantação e manutenção do Programa de Integridade ficam a cargo da Contratada, não cabendo à Empresa Maranhense de Administração Portuária-EMAP o seu ressarcimento
16.6. O Programa de Integridade que seja meramente formal e que se mostre absolutamente ineficaz para mitigar o risco de ocorrência de atos lesivos previstos na Lei Federal nº 12.846, de 2013, não é considerado para fins de cumprimento desta Cláusula.
16.7. Pelo descumprimento das exigências referidas na Lei Ordinária nº 11.463, de 04 de maio de 2021, a Empresa Maranhense de Administração Portuária-EMAP poderá aplicar à Contratada multa equivalente a 0,08%, por dia, incidente sobre o valor atualizado do contrato, limitado a 10% do valor atualizado do contrato.
16.7.1 A aplicação das penalidades pelo descumprimento das exigências de implantação do Programa de Integridade previstas na Lei Ordinária nº 11.463, de 04 de maio de 2021, realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto na referida Lei.
16.7.2 O cumprimento das exigências estabelecidas nesta Cláusula, mediante atestado do órgão ou entidade pública quanto à existência e aplicação do Programa de Integridade, faz cessar a aplicação da multa.
16.7.3 O não cumprimento da obrigação de pagamento da multa no prazo estabelecido implica:
16.7.3.1. inscrição em dívida ativa, em nome da pessoa jurídica sancionada;
16.7.3.2. sujeição a rescisão unilateral da relação contratual, a critério da EMAP;
16.7.3.3. impedimento de contratar com a Empresa Maranhense de Administração Portuária-EMAP, até a efetiva comprovação de implementação do Programa de Integridade, sem prejuízo do pagamento da multa aplicada.

CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO
17.1 Incumbirá à Contratante providenciar a publicação deste instrumento, por extrato, na imprensa oficial.

CLÁUSULA DÉCIMA OITAVA – DA LEGISLAÇÃO
18.1 O presente contrato regula-se por suas cláusulas, pela Lei nº 13.303/2016, pelo Regulamento de Licitações e Contratos, pelo Código de Conduta, pela Política de Integridade, pelo Guia de Clientes e Fornecedores, pela Política de Transação com Partes Relacionadas, todos documentos produzidos pela Empresa Maranhense de Administração Portuária, publicados no site institucional (*www.emap.ma.gov.br*), seção *Transparência*, subseção *Compliance*, e por outras leis, quando couber.

CLÁUSULA DÉCIMA NONA– DA VINCULAÇÃO
19.1 Integram o presente contrato, com força de cláusula contratual, gerando direitos e obrigações, o Edital e respectivos anexos, a proposta do Contratado e a(s) ordem(ns) de fornecimento.
19.1.1 Os documentos referidos na presente cláusula são considerados suficientes para, em complemento a este contrato, definir a sua extensão e intenção, e, dessa forma, reger a execução adequada do objeto contratual.

19.1.2 No caso de dúvida e/ou divergência entre os documentos integrantes do contrato, prevalecerão as condições constantes no edital de licitação.
19.2 O presente contrato tem como fundamento a Lei nº 13.303/2016 e o Regulamento de Licitações e Contratos da EMAP.

CLÁUSULA VIGÉSIMA – DOS CASOS OMISSOS
20.1 Os casos omissos serão decididos segundo as disposições contidas na Lei nº 13.303/2016, no Regulamento de Licitações e Contratos e no Código de Conduta da Empresa Maranhense de Administração Portuária, na Lei nº 8.078/1990 (Código de Defesa do Consumidor) e nas normas e princípios gerais dos contratos.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO FORO
21.1 As partes contratantes elegem o foro de São Luís, Maranhão, 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.

CLÁUSULA VIGÉSIMA SEGUNDA– DA ASSINATURA
22.1. A data de celebração deste instrumento será correspondente a da aposição da última assinatura eletrônica de qualquer das PARTES.

E, por estarem justas e contratadas, assinam as partes, depois de lido e achado conforme, o presente contrato em três vias de igual teor, para a sua validade e eficácia jurídicas.

São Luís, DD de MMMMM de AAAA.

_____ _____

Presidente da EMAP Diretoria da EMAP

_____

Representante Legal da **CONTRATADA**

Testemunhas:

_____ _____

CPF: CPF:

RG: RG:

PREGÃO ELETRÔNICO N° 021/2024 – EMAP

ANEXO VIII

NORMAS DE MEIO AMBIENTE E SEGURANÇA DO TRABALHO PARA EMPRESAS CONTRATADAS E PRESTADORAS DE SERVIÇO NO PORTO DO ITAQUI

01 - OBJETIVO

Estas instruções visam orientar e definir procedimentos para as Empresas Contratadas, no que se refere às diretrizes Básicas de Segurança do Trabalho, Higiene Industrial na área do Porto Organizado do Itaqui, com o objetivo de preservar a integridade do trabalhador, meio ambiente e o patrimônio, assegurando a continuidade das atividades.

02 - CONCEITUAÇÃO

Para os fins desta Norma, Empresas e Contratadas ou, simplesmente Contratados, são as empresas que, mediante um instrumento contratual, executem serviços para a EMAP e tenham empregados trabalhando nas dependências da mesma.

Prestadoras de Serviço são todas as empresas que prestam serviços nas áreas sobre administração da EMAP, incluindo: Operadores, Arrendatários e prestadores de serviço.

03 - APLICAÇÃO

Estas instruções aplicam-se às Empresas referidas no item 02 e devem, obrigatoriamente, ser parte integrante dos Editais de Licitação e anexo ao contrato.

Na execução do objeto do contrato, obrigam-se, ainda, as Contratadas a respeitar a legislação vigente sobre a Engenharia de Segurança e Medicina do Trabalho, Portaria 3214/78, Programa de Gerenciamento de Segurança e Saúde Ocupacional, acatando, também, outras recomendações específicas que sejam feitas pela COSET – Coordenadoria de Saúde e Segurança do Trabalho.

04 - CONDIÇÕES GERAIS E ESPECÍFICAS

4.1 - Precauções

A Contratada juntamente com o fiscal do contrato (EMAP), deverá comparecer junto a Coordenadoria de Saúde e Segurança do Trabalho - COSET, antes do início das obras ou serviços, a fim de tomarem ciência das medidas a serem adotadas durante a execução dos mesmos.

Apresentar os seguintes documentos:

DOCUMENTOS	PRAZO
PCMAT	Até 48 horas antes de iniciar os serviços
PCMSO	Até 48 horas antes de iniciar os serviços
Exames médicos e ASO	Antes do início dos serviços
Certificado de treinamento 6 (seis horas)	Antes do início dos serviços
Vínculo empregatício	Antes do início dos serviços
Relação de EPI´S com os CA'S	Antes do início dos serviços

4.2 - Vistorias de Segurança

A COSET realizará, podendo ter o acompanhamento dos membros da CIPA, no desempenho de suas funções inspeções periódicas nos canteiros de obras/serviços da Contratada, visando verificar o cumprimento das determinações legais referentes à Engenharia de Segurança e Medicina do Trabalho e Meio Ambiente, assim como normas, instruções, recomendações e outros atos da EMAP sobre o assunto.

Constatadas quaisquer irregularidades, a COSET, CIPA e demais empregados da EMAP, deverão notificar o Fiscal do Contrato, que providenciará para que sejam sanadas as irregularidades apontadas, sob pena de aplicação das penalidades cabíveis.

A EMAP poderá a qualquer tempo, solicitar a presença de representantes da Superintendência Regional do Trabalho - SRT, em suas obras, a fim de auxiliar na orientação e fiscalização do cumprimento de todas as disposições legais.

Além dos relatórios que a Contratada está obrigada a fornecer ao Ministério do Trabalho, conforme legislação vigente, obriga-se também a enviar mensalmente a EMAP, o Relatório Mensal de Acidentes. Os Relatórios deverão ser enviados a COSET, no máximo até o 3º dia útil do mês subsequente, conforme Ficha de Controle de Acidentes do PSSO.

Obs. A ocorrência de qualquer acidente deve ser comunicado a COSET de imediato (mesmo turno da ocorrência), através do telefone 3216 -6053 e 3216-6087.

4.3 - Suspensão dos Trabalhos por Motivo de Segurança

4.3.1 - A EMAP se reserva o direito de suspender qualquer trabalho em que se evidencie risco iminente de ameaça à segurança e/ou danos às pessoas, bem como no ambiente de trabalho, ficando estabelecido que estas suspensões não eximem a Contratada das obrigações e penalidades estabelecidas no Contrato, referentes a prazos e multas.

4.3.2 - O não cumprimento das Normas acarretará à Contratada a suspensão de medições, pagamentos e/ou serviços pela EMAP, sem prejuízo das obrigações e penalidades contratuais referentes a prazo.

05 - CIPA

Conforme o quadro I da NR5, a Contratada procederá da forma abaixo.

5.1.1 - Com número inferior a 20 (vinte) empregados, deverá escolher um **responsável** pelo **cumprimento** das atribuições da NR 05 e, consequentemente oficializá-los perante a COSET e CIPA da EMAP.

5.1.2 - Com número igual ou superior a 20 (vinte) empregados deverá formar sua CIPA e, oficializá-la em 30 dias após mobilizações dos canteiros de obra.

Nota:

As Contratadas deverão apresentar a COSET e CIPA evidências objetivas de suas CIPA's, obedecendo rigorosamente a NR 05. Também deverá constar programa de conscientização de seus empregados, quanto à prática de segurança, por exemplo: reuniões periódicas, campanhas, treinamentos, etc.

06 - SESMT

6.1- As Contratadas deverão possuir Serviço Especializado em Segurança e Medicina do Trabalho – SESMT, de acordo com o Quadro I, da NR 4, Portaria 3.214/78.

6.2 - As Contratadas deverão apresentar registro profissional dos integrantes de seus respectivos SESMT na SRT à COSET.

07. TREINAMENTO DE SEGURANÇA

As Contratadas que possuírem o SESMT deverão apresentar cronograma de treinamento, contendo local, conteúdo programático, carga horária, antes do início das atividades na EMAP. Após realização dos cursos deverão ser enviadas as listas de presença para a COSET.

O treinamento ministrado pelo SESMT das Contratadas deverá conter no mínimo o conteúdo e carga horária do programa definido na NR 18.

Quando necessário a COSET, convocará novamente os empregados das Contratadas para o treinamento de reciclagem.

O Crachá definitivo para acesso a EMAP só será reconhecido após conclusão do curso citado acima, onde a COSET emitirá selo de validade.

8 - PROGRAMA DE GERENCIAMENTO DE SEGURANÇA DO TRABALHO – PGSSO.

As Contratadas obrigatoriamente deverão fazer uso das ferramentas de prevenção de acidentes, constantes do Programa de Gestão de Segurança e Saúde Ocupacional da EMAP.

9 - EQUIPAMENTOS DE PROTEÇÃO INDIVIDUAL – EPI's

A partir do Portão de acesso a área primária os empregados deverão fazer uso obrigatório de **capacete de segurança, botina de segurança e óculos de segurança**, não sendo permitido o acesso a pé sem uso dos mesmos.

9.1 - É obrigação da Contratada envidar todos os esforços no sentido de eliminar quaisquer riscos de acidentes e danos à saúde de seus empregados, através de medidas de proteção coletiva.

9.2 - Quando as medidas de proteção coletiva forem tecnicamente inviáveis, ou não oferecerem completa proteção aos empregados, ou enquanto estas medidas estiverem sendo implantadas e/ou em situações de emergência, a Contratada obriga-se a fornecer aos seus empregados Equipamentos de Proteção Individual - **EPI's,** conforme NR 6 da portaria 3.214 de 08.06.1978.

9.3 - As Contratadas deverão treinar seus empregados quanto ao uso dos EPI's e torná-lo obrigatório.

9.4 - É obrigação da Contratada o fornecimento gratuito aos seus empregados e de Equipamentos de Proteção Individual – EPI's, com certificado de aprovação (CA) emitido pelo Ministério do Trabalho, em perfeito estado de conservação e funcionamento, conforme a norma Regulamentadora NR 06 , da portaria 3.214/78 e/ou normas internas que possam vir a ser estabelecidas pela EMAP.

9.5 - As Contratadas antes do início das atividades deverão apresentar a COSET (Segurança do Trabalho) amostras dos EPI's a serem utilizados, onde o Engenheiro de Segurança analisará, podendo ou não aprová-los.

Os serviços só poderão ser iniciados quando os empregados das Contratadas ou Subcontratadas estiverem equipados com os EPI's adequados.

10 - INSTALAÇÕES PROVISÓRIAS NO CANTEIRO DE OBRAS

10.1 - Não é permitida a construção de qualquer alojamento, escritório de campo, depósito ou barracão em área da EMAP sem a sua autorização, por escrito, através do órgão responsável pela obra.

10.2 - Os alojamentos, escritórios de campo, depósitos ou barracões devem ser identificados com emblemas ou logotipo da Contratada.

10.3 - Os alojamentos, escritórios de campo, devem ser mantidos pintados, limpos, arrumados em perfeitas condições de segurança, cabendo ao fiscal do contrato e a **COSET** e/ou **CIPA** da EMAP, fazer a devida fiscalização.

11 - INSTALAÇÕES SANITÁRIAS/VESTIÁRIOS

A Contratada obriga-se a adquirir ou construir instalações sanitárias no seu canteiro de obras ou áreas de atuação, de conformidade com a legislação vigente, obedecendo as instruções especificadas na NR-18.

12- LOCAL PARA REFEIÇÃO / ÁGUA POTÁVEL

12.1 - A Contratada deve providenciar, em seu canteiro de obras, dependências que atendam aos requisitos de limpeza, arejamento e iluminação, onde seus empregados possam guardar e fazer suas refeições, de forma a atender a NR-18 - Condições e Meio Ambiente de Trabalho na Indústria da Construção - Portaria 3.214.

Nota

Quando houver locais com instalações já definidas para empresas Contratadas, a EMAP, durante a vigência do contrato, colocará aquelas instalações à disposição da Contratada, responsabilizando-a por quaisquer danos às referidas instalações.

13 - RESÍDUOS E ENTULHO DE OBRAS

13.1 A Contratada é responsável pela coleta seletiva de Resíduos e limpeza de entulho de obras em seus acampamentos, escritórios e frentes de serviços, devendo ser obedecidas as Normas Regulamentadora NR-24 e 25, da Portaria 3.124, do Ministério do Trabalho e orientação da COSET (Meio Ambiente).

13.2 É de responsabilidade da Contratada providenciar vasilhames descartáveis e sacos plásticos para coleta e acondicionamento dos resíduos e resto de alimentos, os quais deverão ser destinados a um aterro sanitário, em locais a serem definidos pela fiscalização do contrato e a COSET (Meio Ambiente), onde não houver ponto de coleta de Resíduos.

13.3 Os Resíduos e o entulho de obras só poderão ser depositados na EMAP, nos locais determinado pela gerencia de contrato, podendo ainda a EMAP proibir o depósito em locais fora de sua área uma vez comprovado que a comunidade vizinha possa ser prejudicada.

13.4 A responsabilidade pela manutenção da ordem nos locais de depósito de Resíduos e de entulhos de obras é exclusiva das Contratadas que os utilizam, devendo as áreas ser mantidas permanentemente limpas.

14 - ELETRICIDADE

14.1 A ligação à rede de distribuição de energia elétrica da EMAP somente poderá ser feita pelo Setor de Manutenção da área da EMAP através da solicitação do fiscal do contrato.

14.2 Somente é permitida a execução de serviços em redes de alta tensão, ou próximo às mesmas, após desenergizar o sistema elétrico em questão, com a autorização do Setor de Manutenção da área.

14.3 A troca de fusíveis somente pode ser feita pelo setor de Manutenção da EMAP.

14.4 Qualquer ligamento ou desligamento de painel elétrico, somente poderá ser efetuado pelo setor de Manutenção da EMAP, provido com cartão de bloqueio e solicitado pelo Fiscal do Contrato.

14.5 A execução de instalações elétricas provisórias no canteiro de obras deve atender, quanto à segurança, ao disposto na Norma Regulamentadora nº 18 - Condições e Meio Ambiente de Trabalho na Indústria da Construção e NR 10 - Instalações e Serviços de Eletricidades - com redação dada pela Portaria 3.214.

14.6 Os profissionais da Contratada que exerçam atividades relacionadas com eletricidade deverão atender todas as exigências da NR 10 Instalações e Serviços com Eletricidade e conhecimento da Norma de Bloqueio da EMAP.

15- ÁGUA / ESGOTO / GÁS/ AR COMPRIMIDO

15.1 As ligações de água, esgoto, gás e ar comprimido, somente podem ser executadas pelos órgãos competentes da EMAP, ou sob sua orientação direta.

15.2 Os trabalhos sob ar comprimido devem, obrigatoriamente, obedecer aos dispositivos legais vigentes (NR 15), bem como as Normas oriundas da EMAP.

15.3 - É obrigatório o uso de unidade purificadora de ar comprimido nos serviços de jateamento para trabalhos com duração acima de 02 horas, sendo aconselhável o uso do unificador de ar. A saída do ar para o usuário deve ser feita através de engate rápido, ou por um bico. A regulagem do fluxo do ar pode ser feita no painel de distribuição, ou no conjunto do cinto do usuário.

16 - DEPÓSITO, MANUSEIO, TRANSPORTE E AVISO APROPRIADOS PARA PRODUTOS INFLAMÁVEIS/CORROSIVOS E TÓXICOS.

16.1 O manuseio, transporte, armazenamento e uso de produtos inflamáveis, corrosivos e tóxicos deverão ser feitos de acordo com a Norma Regulamentadora 19, da Portaria 3.214, de 08/06/78, do Ministério do Trabalho. A Contratada será a única responsável por qualquer dano ou consequência de acidentes em quaisquer destas atividades.

16.2 Os depósitos de inflamáveis, corrosivos e tóxicos devem situar-se em locais apropriados, determinados pelo Fiscal do contrato, ouvido a COSET (Segurança do Trabalho), e devidamente protegidos, sinalizados e isolados, de conformidade com a legislação e normas vigentes. A esses locais só deverão ter acesso às pessoas credenciadas e que percebem o Adicional de Periculosidade ou Insalubridade, se devido.

16.3 - O transporte de inflamáveis deve ser feito, obrigatoriamente, em recipientes e/ou carros-tanques apropriados e equipados com extintores de incêndio adequados e devidamente sinalizados.

16.4 - Avisos de "É PROIBIDO FUMAR" e "INFLAMÁVEIS" devem ser colocados em locais de fácil visibilidade, onde haja perigo de presença de vapores ou materiais inflamáveis.

17 - OBRAS DE CONSTRUÇÃO, DEMOLIÇÃO E REPAROS.

17.1- Armazenamento e Estocagem de Materiais

Os materiais empregados nas construções devem ser arrumados de modo a não prejudicar o trânsito de pessoas, a circulação de materiais, o acesso aos equipamentos de combate a incêndio, não obstruir portas ou saídas de emergências e não provocar empuxos ou sobrecargas em paredes ou lajes, além dos previstos em seus dimensionamentos, obedecendo as instruções especificadas na NR-18.

17.2- Demolição

Antes de ser iniciada qualquer obra de demolição, as linhas de abastecimento de energia elétrica, água, gás e as canalizações de esgotos e de escoamento de água devem ser desligadas, retiradas ou protegidas, respeitando-se normas e determinações especificadas na NR-18.

17.3 - Andaimes

Os andaimes devem ser dimensionados e construídos de modo a suportar, com segurança, as cargas de trabalho a que estarão sujeitos, respeitando-se normas e determinações especificadas na NR-18.

17.4 - Manuseio de Materiais e Transporte de Pessoas e de Materiais

Nos trabalhos de aplicação de laminados e pisos fixados por cola, bem como em qualquer trabalho que utilize solvente inflamável ou tóxico, devem respeitar as normas e determinações especificadas na NR-18.

17.5 - Serviço de Jateamento e Pintura

Os serviços de Jateamento devem ser executados dentro da condição de segurança exigida, respeitando as normas e determinações especificadas na NR-18.

18 - PROTEÇÃO CONTRA INCÊNDIO

A Contratada deve dispor de equipamentos de proteção e combate a incêndios, mantidos nas instalações provisórias do canteiro de obras, nos diversos locais de trabalho, veículos e equipamentos de sua propriedade, cuja execução deve estar de acordo com orientação da COSET ((Segurança do Trabalho), respeitando as normas e determinações especificadas na NR-23 e NR 18.

19- NORMAS LEGAIS DE SEGURANÇA EM SERVIÇOS DE CONSTRUÇÃO CIVIL

Visando prevenir acidentes com seus empregados, bem como o pessoal da EMAP que transita ou trabalha em área adjacentes às obras, a Contratada deve, obrigatoriamente adotar as medidas de proteção constantes da Norma Regulamentadora NR 18 - Condições e Meio Ambiente de Trabalho na Indústria da Construção - com redação pela Portaria nº 4/95.

20- PCMSO- PROGRAMA DE CONTROLE MÉDICO E SAÚDE OCUPACIONAL

Contratada deverá proceder aos exames médicos admissionais, periódicos, demissionais, de retorno ao trabalho e de mudança de função, conforme especificado na NR 7 – PCMSO.

21 - COMUNICAÇÃO DE ACIDENTES

21.1- A Contratada deverá comunicar a COSET (Segurança do Trabalho), todo acidente grave ou não que implique lesão pessoal, dano à propriedade perda material ou de tempo ocorrido com o seu pessoal por escrito ou por meio eletrônico, no máximo até 12 horas após o ocorrido.

21.2 - Informar a COSET, a entidade médica à qual deverá ser encaminhado seu pessoal em caso de acidentes do trabalho.

22 - PROTEÇÃO CONTRA AGRESSÃO AMBIENTAL

22.1- Cumprir e fazer cumprir a legislação pertinente ao assunto.

22.2- É terminantemente proibido:

⇒ Lançar quaisquer produtos agressivos (sabão, óleo, combustíveis, detergentes), resíduos líquidos ou sólidos de qualquer espécie, nocivos à vida animal e vegetal em geral, em águas interiores, no solo, no ar e mar.

23 - RESPONSABILIDADE DA CONTRATADA

23.1- Caso haja alguma situação provocada direta ou indiretamente pela Contratada, de forma que as consequências venham recair ou serem incutidas a EMAP, sem prévia consulta relativa ao problema, à Contratada será responsabilizada pelo fato, por omissão de informação.

23.2- As irregularidades encontradas serão notificadas ao Órgão de Contratação, sendo adotadas, conforme a gravidade do problema levantado, medidas cabíveis, podendo inclusive ser efetuadas multas ou rescisão do contrato.

23.3 - Obrigam-se ainda, as Contratadas a respeitar a Legislação vigente sobre Segurança e Medicina do Trabalho, acatando outras recomendações específicas que, nesse sentido, sejam determinadas pela EMAP através da COSET, no documento Contratual.

23.4- A Contratada deverá através do **SESMT e/ou CIPA**, desenvolver as atividades pertinentes às áreas de Segurança e

Medicina do Trabalho de forma a cumprir a Legislação e atender às solicitações da contratante, no caso de inspeção da DRT da Região, incluindo-se, por exemplo, o MAPA DE RISCO AMBIENTAL (NR 9 - com redação dada pela Portaria nº 25 - 29/12/94).

24 - VEÍCULO DE GRANDE PORTE

Todos os veículos de grande porte tais como: moto niveladoras, tratores, pás mecânicas, carregadeiras, caminhões, guindastes e outros deverão possuir sinalização sonora quando estiverem em marcha ré.

24.1 O deslocamento de veículo de grande porte com excesso lateral ou de altura, fora das áreas operacionais, deverão se fazer com o auxílio de batedor e devidamente sinalizado.

25- VISITAS TÉCNICAS

Por ocasião das visitas Técnicas das Contratadas nas áreas operacionais da EMAP, os seus representantes deverão portar e usar equipamentos de proteção individual básicos (capacete, sapato fechado, e óculos de segurança) e outros, conforme recomendação da área.

26 - TRÂNSITO- VEÍCULO MOTORIZADO- TRANSPORTE DE PESSOAS

Os veículos de propriedade da Contratada ou a seu serviço somente podem transitar pelas áreas da EMAP quando devidamente autorizados pelo órgão competente, que deve fornecer identificação especial, a ser afixada em local bem visível desses veículos, respeitando as normas e determinações especificadas na NR-18.

26.1- Transporte de empregados

O transporte de pessoas só poderá ser executado em veículo destinado a esse fim, ficando vedado o transporte em veículo adaptado, carroceria de camionetas etc.

26.2- Crachá

É obrigatório o uso do crachá por parte dos empregados da Contratada, sendo necessário a sua apresentação sempre que solicitados por parte da segurança patrimonial da EMAP.

26.3- Veículos

A Contratada deve informar antes do início da obra a relação de veículos com suas respectivas características: tipo, marcas, cor e placa, todos acompanhados do xerox do DUT e conter a logomarca da empresa ao qual presta serviço.

27 - CONSIDERAÇÕES FINAIS

27.1- A ação ou omissão da EMAP não anula nem invalida a responsabilidade da Contratada, quanto à prevenção e/ou consequência de acidentes ocasionais por seu pessoal, veículos e equipamentos.

27.2- A presente Norma aplica-se igualmente a qualquer outra pessoa física ou jurídica devidamente autorizada pela EMAP ou pela Contratada, que se encontrar dentro de sua área.

27.3- A EMAP se reserva ao direito de modificar ou acrescentar novas exigências sobre Segurança e Medicina do Trabalho sempre que julgar necessário para aperfeiçoamento das condições de segurança e proteção de pessoal, equipamentos, materiais e instalações.

27.4- Relacionamento EMAP/Contratadas - todos os assuntos entre a EMAP e Contratadas deverão ser tratados através do fiscal de Contrato, que terá assistência de todos os órgãos da empresa.

27.5- As Empresas Contratadas deverão conhecer e seguir os Procedimentos de Segurança legais e Normas da EMAP.

27.6- A Contratada deverá elaborar Ordem de Serviço, conforme determina a NR 01, item 1.7 e entregar uma cópia, solicitando conhecimento de todos os seus empregados e enviar um modelo dessa O.S. para a Segurança do Trabalho **da EMAP**.

27.7- As empresas Contratadas, Operadoras Portuárias e Arrendatários que subcontratarem mão de obra, equipamentos e veículos para executar trabalhos na área alfandegada do Porto do Itaqui, deverão garantir boas condições de operacionabilidade dos equipamentos e veículos, bem como, a identificação da empresa tomadora dos serviços nos veículos e equipamentos de forma indelével, bem visível; garantir também que a mão de obra use os EPI's obrigatórios para as áreas operacionais, não sendo permitido o uso de bermudas, chinelos e camisetas.

27.8- Toda e qualquer dúvida pertinente ao assunto, deverá ser dirimida sob consulta à COSET.

Empresa Maranhense de Administração Portuária - EMAP
Porto do Itaqui | São Luís | Maranhão | Brasil
Av. dos Portugueses | s/nº | 65085-370 | Tel.: +55 98 3216-6000
Ouvidoria: (98) 3216-6562 / ouvidoria@emap.ma.gov.br
comunicacao@emap.ma.gov.br | www.emap.ma.gov.br