EDITAL DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 170/2023

PROCESSO Nº 709/2023

O Município de Santa Maria, por meio de seu Pregoeiro, designado pela Portaria n.º 64 de 29 de setembro de 2023, torna público para conhecimento dos interessados, que na data, horário e local abaixo indicados fará realizar licitação na modalidade de **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO POR LOTE**, conforme descrito neste Edital. O procedimento licitatório será regido pela Lei nº 10.520, de 17 de julho de 2002; pelo Decreto nº 3.555, de 08 de agosto de 2000 e alterações posteriores; pelo Decreto nº 10.024, de 20 de setembro de 2019; pela Lei Complementar nº 123, de 14 de dezembro de 2006, alterada pela Lei Complementar nº 147, de 07 de agosto de 2014; pelo Decreto nº 8.538, de 6 de outubro de 2015; pelo Decreto Executivo Municipal nº 071, de 03 de agosto de 2015; pela Lei nº 8.666, de 21 de junho 1993 e alterações posteriores, pelas demais normas específicas aplicáveis ao objeto, ainda que não citadas expressamente, e pelas demais exigências deste Edital e seus anexos.

1. DO OBJETO

1.1. A presente licitação tem por objeto **Contratação de Solução de Segurança da Informação com instalação suporte e serviço de resposta a incidentes (Solução XDR),** conforme Termo de Referência (Anexo I), visando suprir a necessidade da Prefeitura Municipal de Santa Maria/RS, nos termos e condições constantes no presente Edital e seus Anexos.

1.2. Não é permitida a subcontratação do objeto.

2. DO ENDEREÇO, DATA E HORÁRIO DO CERTAME

2.1. A sessão pública deste Pregão Eletrônico será aberta por comando do Pregoeiro com a utilização de sua chave de acesso e senha, no endereço eletrônico, data e horário abaixo discriminados:

ENDEREÇO ELETRÔNICO: https://www.gov.br/compras/pt-br

UASG: 988841- Pregão Eletrônico Nº 170/2023

DATA: 06/12/2023

HORÁRIO: 14h (horário de Brasília)

2.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e endereço eletrônico, salvo comunicação do Pregoeiro em sentido contrário.

2.3. A licitação será em único lote conforme planilha constante no Edital.

2.4. O critério de julgamento adotado será o menor preço do lote, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2.5. Para os itens 01 e 02 será por lotes conforme a seguinte justificativa da Secretaria de Inovação e Tecnologia de Informação:" *A solução proposta, contempla integração entre softwares e serviços, permitindo o monitoramento online das ameaças ao ambiente do datacenter município e a aquisição de um fornecedor garante o conhecimento prévio da configuração/ parametrização das licenças e serviços contratados em casos de necessidade do serviço de monitoramento agir preventivamente."*

3. DA DOTAÇÃO ORÇAMENTÁRIA

3.1. Os recursos orçamentários para a despesa correrão por conta das seguintes dotações orçamentárias:

Secretaria de Município de Inovação e Tecnologia de Informação
Solicitação de Compra n.º 1662/2023
Projeto/Atividade: 2055
Subelemento Despesa: 3.3.90.40.99.00
Recurso: 2500

4. DO CREDENCIAMENTO

4.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

4.1. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

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

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

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

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

5. DAS CONDIÇÕES DE PARTICIPAÇÃO

5.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

a) Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

5.2. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para, nos limites previstos da Lei Complementar nº 123, de 2006.

5.3. Não poderão participar desta licitação:

a) Proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

b) Não poderão participar do certame as empresas que estejam reunidas em consórcio e sejam controladoras, coligadas ou subsidiárias entre si, qualquer que seja sua forma de constituição; Tal vedação deve-se pelo fato de que o objeto não apresenta alta complexidade técnica que impossibilite a participação de empresas de forma individual, nem tampouco de grande vulto, não sendo necessária a junção de empresas para sua perfeita execução, ampliando sobremodo a competitividade do certame.

c) Que não atendam às condições deste Edital e seu(s) anexo(s);

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

e) Que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

f) Que estejam sob falência, concurso de credores, concordata ou em processo de dissolução ou liquidação;

g) Entidades empresariais que estejam reunidas em consórcio;

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

5.4. Como condição para participação no Pregão, a licitante assinalará "sim" ou "não" em campo próprio do sistema eletrônico, relativo às seguintes declarações:

a) Que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

5.4.1.1. Nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame;

5.4.1.2. Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

b) Que está ciente e concorda com as condições contidas no Edital e seus anexos;

c) Que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

d) Que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

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

f) Que a proposta foi elaborada de forma independente.

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

h) Que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

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

6. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação e qualificação técnica exigidos (conforme item 10 deste Edital), a proposta com a descrição do objeto ofertado e o preç**o, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação, conforme art. 26, Decreto nº 10.024/2019.**

6.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

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

6.4. As Microempresas e Empresas de Pequeno Porte **deverão** encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

6.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

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

6.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

7. DO PREENCHIMENTO DA PROPOSTA

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

a) Valor unitário e total do lote;

b) Marca/Modelo;

c) Fabricante;

d) Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável;

7.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

7.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação de serviços.

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

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

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

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

8.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

a) Também será desclassificada a proposta que identifique o licitante.

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

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

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

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

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

a) O lance deverá ser ofertado pelo valor total/unitário do item.

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

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

8.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,1% (zero vírgula um por cento).

8.9. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances.

8.10. Será adotado para o envio de lances no pregão eletrônico o **modo de disputa "aberto"**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

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

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

8.13. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

8.14. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

8.15. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério da Economia;

a) Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

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

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

8.18. 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.

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

8.20. O Critério de julgamento adotado será o **menor preço**, conforme definido neste Edital e seus anexos.

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

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

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

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

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

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

8.27. Quando houver propostas beneficiadas com as margens de preferência em relação ao produto estrangeiro, o critério de desempate será aplicado exclusivamente entre as propostas que fizerem jus às margens de preferência, conforme regulamento.

8.28. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances).

8.29. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

a) No país;

b) Por empresas brasileiras;

c) Por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

d) Por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

8.30. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

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

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

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

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

9. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

9.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

9.2. Será desclassificada a proposta ou o lance vencedor, apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente inexequível.

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

9.3. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

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

9.5. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de **2 (duas) horas**,sob pena de não aceitação da proposta.

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

b) Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

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

9.7. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "*chat*" a nova data e horário para a sua continuidade.

9.8. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

a) Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

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

9.9. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

9.10. Encerrada a análise quanto à aceitação da proposta, o pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

10. DA HABILITAÇÃO

10.1. 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:

a) SICAF;

b) Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/)

c) A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

10.1.3.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

10.1.3.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de prestação de serviços similares, dentre outros.

10.1.3.3. O licitante será convocado para manifestação previamente à sua desclassificação.

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

e) No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

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

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

b) É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

c) O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

10.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **2 (duas) horas**, sob pena de inabilitação.

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

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

10.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

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

10.7. Ressalvado o disposto no item 6.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

10.8. Habilitação Jurídica:

a) No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

c) No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

d) inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

e) No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

f) No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

g) No caso de agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 4º, §2º do Decreto n. 7.775, de 2012.

h) No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

i) Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

10.9. Regularidade Fiscal e Trabalhista:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

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

c) Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

d) Prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

e) Prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

f) Prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

g) Prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

h) Caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

i) Caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

10.10. Qualificação Econômico-Financeira.

10.10.1 Certidão Negativa de Falência ou Recuperação Judicial expedida pelo distribuidor da sede da pessoa jurídica, ou, se for o caso, de Execução Patrimonial, expedida no domicílio da pessoa física.

10.10.2. Demonstrações Contábeis do Último Exercício Social, que comprovem a boa situação financeira da empresa para atender plenamente objeto de potencial contrato de fornecimento de material ou serviço à municipalidade. Os demonstrativos citados deverão estar adequados às seguintes propriedades:

10.10.2.1. Quanto à sua finalidade, os demonstrativos exigidos, devem possibilitar a apuração e avaliação de índices de liquidez e solvência do pleiteante, devendo ser compostos, no mínimo, pelo Balanço Patrimonial e pela Demonstração do Resultado do Exercício.

10.10.2.2. Quanto à sua forma, devem estar adequados à legislação vigente, incluindo-se as Normas Brasileiras de Contabilidade; contendo informação comparativa do exercício imediatamente anterior, Termos de Abertura e Encerramento; adicionando-se, no caso de Escrituração Contábil Digital (ECD), o Recibo de Entrega.

10.10.2.3. Quanto à sua legitimidade, deverá ser comprovado seu registro junto aos órgãos legalmente instituídos para tal fim, como Junta Comercial Estadual ou Cartório de Notas, bem como a Receita Federal do Brasil; de acordo com as regras que enquadrem suas características societárias e/ou fiscais.

10.10.2.4. Quando à sua tempestividade, em caso de constituição da sociedade em período inferior a 12 meses, deverá ser apresentada cópia autenticada do Balanço de Abertura, devidamente registrado ou autenticado na Junta Comercial ou órgão competente.

10.10.3. Memorial de Cálculo contendo a boa situação financeira, avaliada pelos Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), resultantes da aplicação das seguintes fórmulas:

$$LG = \frac{\text{ATIVO CIRCULANTE + ATIVO REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}} \geq 1$$

$$SG = \frac{\text{ATIVO TOTAL}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}} \geq 1$$

$$LC = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}} \geq 1$$

10.10.3.1. Caso o memorial não seja apresentado, a Comissão de Licitação reserva-se o direito de efetuar os cálculos.

10.10.3.2. Se necessária a atualização do balanço, deverá ser apresentado, juntamente com os documentos em apreço, o memorial de cálculo correspondente.

10.10.4. Caso a empresa apresente índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC) inferiores a 01 (um), deverá comprovar ser dotada de capital social ou de patrimônio líquido igual ou superior a 10% (dez por cento) do valor estimado para a contratação. A comprovação será obrigatoriamente feita pelo Ato Constitutivo, Estatuto ou Contrato Social em vigor e devidamente registrado ou pelo balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, conforme disposto no Art. 31, inciso I, da Lei Federal nº 8.666/93.;

10.11. Qualificação Técnica.

10.11.1 7.1. Comprovação de revendedor autorizado do fabricante da solução de segurança baseada em inteligência artificial.:

10.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

10.13. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do Edital.

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

10.14. Caso a proposta mais vantajosa seja ofertada por licitante qualificada como microempresa ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

10.15. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

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

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

10.17. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

10.18. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

10.19. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

10.20. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

11. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

11.1. A proposta final do licitante declarado vencedor deverá ser encaminhada conforme modelo Anexo II, no prazo estipulado pelo Pregoeiro no chat do sistema eletrônico e deverá:

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

b) Conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

11.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

a) Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

11.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

a) Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

11.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

11.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

11.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

12. DOS RECURSOS

12.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo 30 (trinta) minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

12.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

a) Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

b) A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

c) Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de **3 (três) dias** para apresentar as *razões*, **pelo sistema eletrônico**, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem *contrarrazões* também **pelo sistema eletrônico**, em outros **3 (três) dias**, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

12.3. O recurso contra a decisão do Pregoeiro terá efeito suspensivo, no tocante ao item ao qual o recurso se referir, **inclusive quanto ao prazo de validade da proposta, o qual somente recomeçará a contar quando da decisão final da autoridade competente.**

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

12.5. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto e homologará o procedimento licitatório.

12.6. Os autos do processo permanecerão com vista franqueada aos interessados na Prefeitura Municipal de Santa Maria, Superintendência de Compras e Licitações, Rua Venâncio Aires, 2277, Centro, CEP 97010-005 – Santa Maria/RS, em dias úteis, no horário de **07:30 às 13:00**. Não serão reconhecidos os recursos interpostos enviados fora do Sistema Comprasnet.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

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

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

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

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

b) A convocação feita por e-mail ou fac-símile dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

14.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

14.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

15. DA ASSINATURA DO CONTRATO

15.1. Esgotados todos os prazos recursais, a Administração convocará o representante legal da empresa licitante vencedora para, no prazo de 10 (dez) dias após o recebimento do empenho, assinar o contrato, aceitar o instrumento equivalente, sob pena de decair o direito à contratação, nos termos do art. 64, da Lei Federal nº 8.666/93 e sem prejuízo das sanções previstas no art. 81 da mesma Lei.

15.2. Se dentro do prazo a empresa convocada não assinar o Contrato, a Administração convocará as licitantes remanescentes na ordem de classificação das propostas, para a assinatura do mesmo; ou então, revogará a licitação, sem prejuízo da aplicação de penalidade.

15.3. No Contrato a ser assinado com o vencedor da licitação constará às cláusulas necessárias previstas no art. 55 e a possibilidade de rescisão do mesmo, na forma determinada nos art. 77, 78 e 79 da Lei Federal nº. 8.666/93.

16. DO PRAZO E DAS CONDIÇÕES DA PRESTAÇÃO DO SERVIÇO

16.1. **Para o item 1**: o prazo de vigência do contrato será de 36 (trinta e seis) meses consecutivos e ininterruptos, a partir de sua assinatura, podendo o mesmo ser prorrogado por igual período ou rescindido, conforme interesse público, de acordo com a Lei Federal nº 8.666/93 e suas posteriores alterações.

Para o item 2: o prazo de vigência do contrato será de 12 (doze) meses consecutivos e ininterruptos, a partir de sua assinatura, podendo o mesmo ser prorrogado por igual período ou rescindido, conforme interesse público, de acordo com a Lei Federal nº 8.666/93 e suas posteriores alterações

16.2. Os valores propostos serão reajustados, após um ano de vigência, pelo índice acumulado da variação do ICTI (Índice de Custo de Tecnologia da Informação) ou outro índice oficial que vier a substituí-lo.

16.3. O acesso ao serviço deverá ser disponibilizado em até 05 (cinco) dias corridos após o **recebimento da nota de empenho.**

16.4. Produtos entregues por meio de download ou aceso direto a um endereço da internet, a contratada deverá enviar um e-mail para o sti.pmsm@gmail.com , com todas as informações necessárias para realizar a utilização do produto/serviço objeto desta contratação.

16.5. No prazo máximo de 2 (dois) dias, contados da assinatura do contrato, a contratada deverá realizar reunião inicial de gestão do contrato.

16.6. Deverão estar presentes na reunião o preposto e um integrante da equipe técnica da contratada.

16.7 A pauta da reunião deverá abordar o planejamento detalhado da implantação da solução contratada, além das condições contratuais.

16.8 **Os serviços deverão ser prestados em conformidade com as especificações deste Edital e seus anexos**. Sendo constatada qualquer irregularidade, o prestador deverá concluir os serviços dentro das condições ideais, cujo prazo será determinado no ato pelo responsável do recebimento e imediatamente comunicado à Secretaria de Município para que seja(m) adotada(s) a(s) sanção(ões) cabível.

16.9 A Contratada será responsável por realizar uma consultoria e revalidação das regras do Firewall Fortinet FG-1100E, sendo emitido um relatório com as alterações realizadas na configuração. Esta consultoria e revalidação deverá ser feita com base nas orientações fornecidas pela Fortinet na consultoria Incident Readiness.

16.10 A Contratada deverá configurar as seguintes soluções Fortinet.

- FortiAuthenticator com licença SSO;
- FortiTokenMobile;
- FortiAnalyzer;
- FortiClient EMS com função de ZTNA;
- FortiEDR.

16.11 A Contratada será responsável por configurar por completo cada uma das soluções acima especificadas, sendo dado como aceito o funcionamento quando um total de 10% (dez) do total de licenças esteja plenamente em funcionamento. A Contratada deverá fazer um repasse de conhecimento para a

equipe técnica da Contratante de modo que esta possa dar continuidade na implantação para os demais usuários/equipamentos.

16.12 A Contratada será responsável por configurar o FortiAuthenticator para validar os acessos dos usuários remotos que farão uso do FortiTokenMobile, ferramenta esta que ficará instalada em dispositivos móveis.

16.13 A Contratada será a responsável pela implantação do FortiAnalyzer e configuração / customização dos dispositivos fornecidos para o envio de logs para esta ferramenta de análise.

16.14 A Contratada será responsável por implantar o FortiClient EMS de modo que os usuários externos tenham uma segurança no acesso via esta ferramenta de confiança zero, a qual fará a validação de conformidade de dispositivos e usuários no acesso remoto.

16.15 A Contratada deverá criar templates, configurar servidores, máquinas e profiles do FortiEDR.

16.16 Deverá ser fornecido pela Contratada um treinamento de todas as soluções fornecidas, por um profissional com certificação mínima NSE7, com carga horária mínima de 24 (vinte e quatro) horas, para uma turma de até 6 (seis) pessoas.

16.17 O projeto deverá ser gerenciado por profissional Gerente de Projetos com certificação PMP do PMI ou com pós-graduação em Gerenciamento de Projetos.

16.18 O projeto deverá ser implantado por profissional com certificação mínima NSE7 do fabricante Fortinet.

16.19 A Contratada deverá considerar a participação presencial no projeto por no mínimo 5 (cinco) dias de um profissional com certificação Fortinet conjunto com o Gerente de Projetos para entendimento e consultoria inicial do ambiente envolvido neste projeto.

17. DA FISCALIZAÇÃO

17.1. O acompanhamento e a fiscalização do objeto desta Licitação serão exercidos por meio de um representante (Fiscal do Contrato) e um substituto, designados pela Contratante, aos quais compete acompanhar, fiscalizar, conferir e avaliar a execução do objeto, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando o que for necessário à regularização das faltas, falhas, problemas ou defeitos observados, e os quais de tudo darão ciência à Contratada, conforme determina o art. 67, da Lei nº 8.666/1993, e suas alterações.

a) A fiscalização deverá ser de acordo com o regramento estipulado no Termo de Referência.

17.2. Não obstante ser a Contratada a única e exclusiva responsável pela execução do objeto, a Contratante reserva-se o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização.

17.3. Cabe à Contratada atender prontamente e dentro do prazo estipulado quaisquer exigências da fiscalização inerentes ao objeto desta licitação, **sem que disso decorra qualquer ônus extra para a CONTRATANTE**, não implicando essa atividade de acompanhamento e fiscalização qualquer exclusão ou redução da responsabilidade da Contratada, que é total e irrestrita em relação ao objeto executado, inclusive perante terceiros, respondendo a mesma por qualquer falta, falha, problema, irregularidade ou desconformidade observada na execução do ajuste.

a) A atividade de fiscalização não resultará, tampouco, e **em nenhuma hipótese**, em corresponsabilidade da Contratante ou de seus agentes, prepostos e/ou assistentes.

17.4. O objeto do presente Edital deverá estar rigorosamente dentro das normas vigentes e das especificações estabelecidas pelo Município, sendo que a inobservância desta condição implicará a sua

recusa, bem como sua devida adequação e/ou substituição, sem que caiba à Contratada qualquer tipo de reclamação ou indenização.

17.5. As decisões e providências que ultrapassem a competência da fiscalização serão encaminhadas à autoridade competente da Contratante para adoção das medidas convenientes, consoante disposto no § 2º do art. 67, da Lei nº. 8.666/93.

18. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

18.1. **CABERÁ À CONTRATADA**, sem prejuízo das demais obrigações e responsabilidades insertas neste Edital e daquelas constantes do Termo de Referência (**Anexo I deste Edital**):

a) Tomar todas as providências necessárias à fiel execução do objeto desta licitação;

b) Promover a execução do objeto dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações ac

c) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto deste Contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução do serviço;

d) Manter durante a execução deste contrato todas as condições de habilitação e qualificação exigidas na licitação;

e) Responsabilizar-se pelas despesas decorrentes de frete, seguro e demais encargos;

f) Entregar o objeto a ser contratado, conforme convencionado, sem qualquer outro encargo ou despesa para o Contratante.

g) Se for o caso, a Contratada deverá fornecer informações contendo nome completo, CPF, cargo ou atividade exercida, lotação e local de exercício dos empregados na Contratante, para fins de divulgação na internet.

h) Prestar todos os esclarecimentos que lhe forem solicitados pela Contratante, atendendo prontamente a quaisquer reclamações;

i) Arcar com os ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de contravenção, seja por culpa sua ou de quaisquer de seus empregados ou prepostos, obrigando-se, outrossim, a quaisquer responsabilidades decorrentes de ações judiciais ou extrajudiciais de terceiros, que lhe venham a ser exigidas por força da lei, ligadas ao cumprimento do ajuste a ser firmado;

j) Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com a Contratante;

k) Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados quando da execução do objeto ou em conexão com ele, ainda que acontecido em dependência da Contratante, inclusive por danos causados a terceiros;

l) Obedecer às normas de segurança e higiene no trabalho e o fornecimento de todo o equipamento de proteção individual - EPI, necessário ao pessoal utilizado na prestação dos serviços.

19.1.12.1. Fornecimento de vestimenta de trabalho e de todo o equipamento de proteção coletiva - EPC, necessário ao pessoal utilizado na prestação dos serviços;

m) Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionados à execução do objeto, originariamente ou vinculada por prevenção, conexão ou contingência;

n) Assumir a responsabilidade pelos encargos fiscais, comerciais e tributários resultantes da adjudicação deste processo licitatório;

o) Respeitar fielmente as Políticas, e Normas e Procedimentos de Segurança da Informação da Contratante.

p) Fornecer todos os materiais necessários à perfeita utilização dos equipamentos;

q) Não efetuar, sob nenhum pretexto, a transferência de qualquer responsabilidade para outras entidades, seja fabricantes, técnicos, subempreiteiros etc., sem a anuência expressa e por escrito da área administrativa da CONTRATANTE;

r) Responsabilizar-se pelo credenciamento e descredenciamento de acesso às dependências da CONTRATANTE, assumindo quaisquer prejuízos porventura causados por seus recursos técnicos;

s) Solicitar, por escrito, credenciamento e autorização de acesso para os recursos técnicos da Prefeitura Municipal de Santa Maria;

t) À CONTRATADA é vedado prestar informações a terceiros sobre a natureza ou andamento do fornecimento, objeto do Contrato, ou divulgá-los através da imprensa escrita, falada, televisada e/ou outro meio qualquer de divulgação pública, salvo autorização expressa da CONTRATANTE;

u) A Contratada deverá cumprir integralmente a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), no que couber.

v) Aceitar, nas mesmas condições do ajuste, os acréscimos ou supressões que se fizerem no objeto, de até 25% (vinte e cinco por cento) de seu valor;

18.2. CABERÁ A CONTRATANTE, sem prejuízo das demais disposições inseridas neste Edital e daquelas constantes do Termo de Referência **(Anexo I deste Edital**):

a) Supervisionar a execução do objeto do Termo de Referência, exigindo presteza na execução e correção das falhas eventualmente detectadas;

b) Prestar à Contratada, em tempo hábil, as informações eventualmente necessárias à execução do objeto.

c) Impedir que terceiros executem o objeto deste Edital;

d) Atestar as faturas correspondentes, por intermédio de servidor competente;

e) Efetuar o pagamento devido pela execução do objeto, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas.

19. DO PAGAMENTO

19.1 O pagamento será efetuado em:

* 15 (quinze) dias consecutivos do recebimento da Nota Fiscal pelo fiscal do contrato. Para tanto a referida fatura deverá estar devidamente visada pelo responsável da Secretaria requisitante e entregue em até 05 dias para a Secretaria de Município de Finanças.

19.1.1 Deverá constar obrigatoriamente nas notas fiscais/faturas o número do empenho.

19.2 O pagamento será creditado em conta corrente da empresa, através de Ordem Bancária contra qualquer instituição bancária indicada na proposta, devendo para isto ficar explicitado o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

19.2.1 Os pagamentos serão concretizados em moeda vigente do país.

19.3 Para execução do pagamento de que trata este subitem, a Contratada deverá fazer constar como beneficiário/cliente da Nota Fiscal/Fatura correspondente, emitida sem rasuras, o Município de Santa Maria, CNPJ n.º 88.488.366/0001-00.

19.4 O pagamento somente será liberado após o recolhimento de eventuais multas que lhe tenham sido impostas em decorrência de inadimplência contratual.

19.5 Qualquer erro ou omissão havidos na documentação fiscal ou na fatura será objeto de correção pela empresa e haverá, em decorrência, suspensão do prazo de pagamento até que o problema seja definitivamente regularizado.

19.6 O Município reserva-se o direito de recusar o pagamento se, no ato do atesto, o objeto licitado não estiver de acordo com a especificação apresentada e aceita no Termo de Referência.

19.1. Na hipótese de atraso no pagamento da Nota Fiscal devidamente atestada, ao valor devido serão acrescentados juros calculados *pro rata die,* de acordo com a variação do **Índice Nacional de Preços ao Consumidor Amplo - IPCA**, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística - IBGE..

20. DAS SANÇÕES ADMINISTRATIVAS

20.1. Se no decorrer da **sessão pública da licitação** ou **na execução do objeto** do presente Edital, ficar comprovada a existência de qualquer irregularidade ou ocorrer inadimplemento pelo qual possa ser responsabilizada a Licitante/Contratada, esta, sem prejuízo das demais sanções previstas nos arts. 86 a 88, da Lei nº 8.666/93, poderá sofrer as seguintes penalidades:

a) Advertência por escrito;

b) Multa de até 10% (dez por cento), calculada sobre o valor total da proposta ou lance ofertado pela LICITANTE DESISTENTE devidamente atualizado, na hipótese de **desistência injustificada** do lance, **após o ENCERRAMENTO da fase de lances**, sem prejuízo da aplicação de outras sanções previstas no art. 49, do Decreto nº 10.024/2019, inclusive de **impedimento de licitar e contratar com a Administração**, previsto no subitem 20.5 deste Edital;

c) Multa de até 5% (cinco por cento) sobre o valor total do contrato (ou documento que o substituir) no caso de inexecução parcial e 10% (dez por cento) sobre o valor total do contrato (ou documento que o substituir), no caso de inexecução total do objeto contratado.

d) Multa de até 10% (dez por cento) sobre o valor total da contratação devidamente atualizado quando for constatado o descumprimento de qualquer obrigação prevista neste Edital e/ou no Termo de Referência;

e) Multa de até 20% (vinte por cento) sobre o valor total da contratação quando for constatada a **reincidência** no descumprimento de qualquer obrigação prevista neste Edital e/ou no Termo de Referência;

f) Pelo **atraso injustificado para a entrega** e/ou **inobservância de outros prazos definidos no Termo de Referência**, multa de 0,33% (zero vírgula trinta e três por cento) incidente sobre o valor total da contratação, por dia de atraso, **a ser cobrada pelo período máximo de 30 (trinta) dias**. **A partir do 31º (trigésimo primeiro) dia de atraso, a contratação poderá ser rescindida**;

20.2. A aplicação das sanções previstas neste Edital não exclui a possibilidade de aplicação de outras, previstas na Lei nº 8.666/1993 e no art. 49, do Decreto nº 10.024/2019, inclusive a responsabilização da licitante vencedora por eventuais perdas e danos causados ao Município de Santa Maria.

20.3. A multa deverá ser recolhida no **prazo máximo de 10 (dez) dias corridos**, a contar da data do recebimento da comunicação enviada pelo Município de Santa Maria.

20.4. O valor da multa poderá ser descontado da Nota Fiscal/Fatura ou de crédito existente no Município de Santa Maria, em favor da Contratada, sendo que, caso o valor da multa seja superior ao crédito existente, a diferença será cobrada na forma da lei.

20.5. A licitante que, convocada no prazo de validade da sua proposta, deixar de executar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do objeto desta licitação, não mantiver a proposta/lance, falhar ou fraudar na execução do objeto, comportar-se de modo inidôneo ou cometer fraude fiscal, **ficará impedida de licitar e contratar com a Administração, além de ser descredenciada do SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste Edital e das demais cominações legais.**

20.6. As sanções previstas neste Edital são **independentes entre si**, podendo ser aplicadas de forma **isolada ou cumulativamente**, sem prejuízo de outras medidas cabíveis.

20.7. Não será aplicada multa se, **justificada e comprovadamente**, o atraso na execução do objeto advier de caso fortuito ou de força maior.

20.8. A atuação da Contratada no cumprimento das obrigações assumidas será registrada no Sistema Unificado de Cadastro de Fornecedores – **SICAF**, conforme determina o § 2º do art. 36 da Lei n.º 8.666/1993.

20.9. Em qualquer hipótese de aplicação de sanções, serão assegurados à licitante vencedora o contraditório e a ampla defesa.

21. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

21.2. As impugnações deverão ser enviadas ao Pregoeiro, **preferencialmente por meio eletrônico**, via internet, no seguinte endereço: pregaoeletronicosm@gmail.com

21.3. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até **dois dias úteis** contados da data de recebimento da impugnação.

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

21.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, **até 03 (três) dias úteis** anteriores à data designada para abertura da sessão pública, **preferencialmente por meio eletrônico**, via internet, no seguinte endereço: pregaoeletronicosm@gmail.com

21.6. O pregoeiro responderá aos pedidos de esclarecimentos no prazo de **dois dias úteis**, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos anexos.

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

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

21.8. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

22. DAS DISPOSIÇÕES GERAIS

22.1. 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 documentos ou informação que deveria constar originariamente. Podendo desconsiderar excessos de formalismos que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

a) A inobservância do prazo fixado pelo Pregoeiro para a entrega das respostas e/ou informações solicitadas em eventual diligência ou ainda o envio de informações ou documentos considerados insuficientes ou incompletos ocasionará a desclassificação da proposta.

22.2. Fica assegurado a Prefeitura Municipal de Santa Maria o direito de, no seu interesse, anular ou revogar, a qualquer tempo, no todo ou em parte, a presente licitação, dando ciência às participantes, na forma da legislação vigente.

22.3. As proponentes assumem todos os custos de preparação e apresentação de suas Propostas e a Prefeitura Municipal de Santa Maria não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

22.4. As proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

22.5. Os documentos apresentados deverão estar em nome da licitante e datados dos últimos 180 (cento e oitenta) dias até a data de abertura da sessão de licitação, quando não tiver prazo estabelecido pelo órgão/empresa competente expedidor(a) e não tiver cadastrado no SICAF.

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

22.7. Em caso de divergência entre as especificações do objeto insertas no Sistema SIASG e as deste Edital, prevalecerão as constantes neste último.

22.8. O desatendimento de exigências formais não essenciais não importará o afastamento da licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua Proposta, durante a realização da sessão pública desta licitação.

22.9. As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança do futuro contrato.

22.10. As licitantes, após a publicação oficial deste Edital, ficarão responsáveis pelo acompanhamento das eventuais republicações e/ou retificações de Edital, respostas a questionamentos e impugnações ou quaisquer outras ocorrências que porventura possam ou não implicar em mudanças nos prazos de apresentação da proposta e da abertura da sessão pública.

22.11. Aos casos omissos aplicar-se-ão as demais disposições constantes na Lei nº 10.520, de 17 de julho de 2002, Decreto Municipal n.° 71/2015 e, subsidiariamente, na Lei n.º 8.666/1993.

22.12. As questões relativas ao presente Edital, que não possam ser dirimidas administrativamente, serão processadas e julgadas no Foro da Comarca de Santa Maria - RS, com exclusão de qualquer outro, por mais privilegiado que seja.

Santa Maria, 22 de novembro de 2023.

Jane Arlene Munhoz Walter
Pregoeira

ANEXO I

TERMO DE REFERÊNCIA

SOLUÇÃO XDR

TRS-2023-24-02

1. OBJETO

Contratação Solução de segurança da informação com instalação suporte e serviço de resposta a incidentes, conforme especificação técnica.

1.1. Quantitativos

Item	Descrição	Quant.	Un.
1	Solução XDR baseado em inteligência artificial com instalação, configuração e suporte, para 36 meses.	5.000	Serviço
2	Serviço de assistência personalizada a incidentes, para 12 meses.	1	Serviço

1.2. Composição da Solução de Segurança baseada em Inteligência Artificial

A solução de segurança deverá contemplar todos os itens e quantidades indicadas abaixo:

	Part-number	Descrição	Qtd
1	FN-FAC-VM-BASE	FortiAuthenticator - VM License	1
2	FN-FAC-VM-1000-UG	FortiAuthenticator - VM License Adds 1,000 users to FortiAuthenticator-VM	2
3	FN-FC3-10-0ACVM-248-02-36	FortiAuthenticator - VM License 24x7 FortiCare Contract (1 - 5100 USERS)	1
4	FN-FCC-FAC2K-LIC	FortiClient SSO License for FortiAuthenticator	1
5	FN-FTM-ELIC-2000	FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 2000 users. Electronic license certificate.	1
6	FN-FC2-10-AZVMS-465-01-36	FORTIANALYZER-VM SUBSCRIPTION LICENSE WITH SUPPORT 3 YEAR SUBSCRIPTION LICENSE FOR 50 GBDAY CENTRAL LOGGING ANALYTICS. INCLUDE 24X7 FORTICARE SUPPORT, IOC, SOC SUBSCRIPTION, AND FORTIGUARD OUTBREAK ALERT SERVICE.	1
7	FN-FC3-10-EMS05-428-01-36	FORTICLIENT - VPN ZTNA 3 YEAR FORTICLIENT VPNZTNA AGENT SUBSCRIPTIONS EMS HOSTED BY FORTICLOUD WITH 24X7 FORTICARE FOR 2000 ENDPOINTS.	2
8	FN-LIC-IR-10	TEN SERVICE POINT FOR IR SERVICES TEN SERVICE POINT FOR IR SERVICES	

9	FN-FP-10-PS001-831-01-01	PER-DAY SOLUTION ARCHITECT CONSULTANCY ENGAGEMENT TO DOCUMENT, DESIGN AND DELIVER SECURITY ARCHITECTURE IMPROVEMENTS PER AGREED SCOPE BOUND BY FORTICARE CONTRACT AND ASSOCIATED TERMS	1
10	FN-FC3-10-FEDR1-349-01-12	FORTIEDR DISCOVER, PROTECT RESPOND AND STANDARD MDR 1 YEAR FORTIEDR DISCOVER, PROTECT RESPOND AND STANDARD MDR SUBSCRIPTION AND 24X7 FORTICARE FOR 2,000 ENDPOINTS	5
11	FN-FP-10-PS001-806-02-03	FortiEDR JumpStart Remote FortiEDR jumpstart support service - up to 3K endpoints	2
12	FN-FP-10-EDR-PS	FortiEDR professional services day	1

1.3. Composição do serviço de resposta a incidentes:

	Part-number	Descrição	Qtd
1	FN-FP-10-IR001-709-02-12	FORTIGUARD INCIDENT READINESS SUBSCRIPTION SERVICE 1 YEAR FORTIGUARD INCIDENT READINESS SUBSCRIPTION SERVICE - 12 MONTHS	1

2. JUSTIFICATIVA

2.1. Para definição da Marca

Considerando a evolução dos riscos diário de segurança da informação, da crescente variedade das formas de violação de segurança que um datacenter pode sofrer diariamente e o encerramento do contrato nº 92/2019 responsável pela atualização das licenças de antivírus.

A equipe técnica optou por buscar no mercado soluções de segurança baseadas em inteligência artificial EDR/XDR, realizando POC de algumas soluções e a que se mostrou mais adequada ao ambiente atual do município é a FortiXDR que apresenta total compatibilidade com o Firewall adquirido pelo Município em setembro de 2022 via Pregão Eletrônico nº 97/2022 que possui licenciamento ativo que poderá ser adicionado a solução pretendida.

Ainda, a indicação da marca segue as orientações de soluções de tecnologia Gartner, a melhor abordagem para proteger ambiente de tecnologia, principalmente considerando funcionários remotos, é através de uma arquitetura chamada CSMA (Cyber Security Mesh Architecture). Existindo uma integração entre as mais diferentes ferramentas, permitindo a correlação dos eventos, bloqueio mais rápido das ameaças e um menor tempo de identificação da ameaça (MTTD) e menor tempo para resolução (MTTR).

Por fim, a solução Fortinet possui atendimento também a segurança de ambientes legados, ou seja, sistemas que utilizam sistemas operacionais fora da vida útil do fabricante (end-of-life), pois o nosso

parque de máquinas possui ainda, computadores com Windows 7 e servidores com Windows Server 2003 e Windows Server 2008 em funcionamento.

Portanto, a solução proposta foi escolhida para garantir a preservação dos investimentos anteriores, pois trata-se de solução no mesmo padrão dos já instalados, o que potencializa a utilização dos atuais por todo o tempo de vida de cada dispositivo. Além do fator econômico, é importante destacar que a solução proposta facilitará a interoperabilidade entre os componentes, o gerenciamento centralizado, a economia de escala e o aproveitamento do conhecimento da equipe técnica.

2.2. Para o lote único

A solução proposta, contempla integração entre softwares e serviços, permitindo o monitoramento online das ameaças ao ambiente do datacenter município e a aquisição de um fornecedor garante o conhecimento prévio da configuração/ parametrização das licenças e serviços contratados em casos de necessidade do serviço de monitoramento agir preventivamente.

3. ENTREGA

3.1. O acesso ao serviço deverá ser disponibilizado em até 5 dias corridos após o **recebimento da nota de empenho.**

3.2. Produtos entregues por meio de download ou aceso direto a um endereço da internet, a contratada deverá enviar um e-mail para o sti.pmsm@gmail.com, com todas as informações necessárias para realizar a utilização do produto/serviço objeto desta contratação.

3.3. No prazo máximo de 2 (dois) dias, contados da assinatura do contrato, a contratada deverá realizar reunião inicial de gestão do contrato.

3.4. Deverão estar presentes na reunião o preposto e um integrante da equipe técnica da contratada.

3.5. A pauta da reunião deverá abordar o planejamento detalhado da implantação da solução contratada, além das condições contratuais.

4. FORMA DE PAGAMENTO

4.1. Pagamento único em até 15 (quinze) dias do recebimento da Nota Fiscal.

5. PERÍODO DE EXECUÇÃO DO CONTRATO

5.1. ***Para o item 1***: o prazo de vigência do contrato será de 36 (trinta e seis) meses consecutivos e ininterruptos, a partir de sua assinatura, podendo o mesmo ser prorrogado por igual período ou rescindido, conforme interesse público, de acordo com a Lei Federal nº 8.666/93 e suas posteriores alterações.

5.2. ***Para o item 2***: o prazo de vigência do contrato será de 12 (doze) meses consecutivos e ininterruptos, a partir de sua assinatura, podendo o mesmo ser prorrogado por igual período ou rescindido, conforme interesse público, de acordo com a Lei Federal nº 8.666/93 e suas posteriores alterações.

5.3. Os valores propostos serão reajustados, após o período de vigência, pelo índice acumulado da variação do ICTI (Índice de Custo de Tecnologia da Informação) ou outro índice oficial que vier a substituí-lo.

6. INSTALAÇÃO E CONFIGURAÇÃO

6.1. A Contratada será responsável por realizar uma consultoria e revalidação das regras do Firewall Fortinet FG-1100E, sendo emitido um relatório com as alterações realizadas na configuração. Esta consultoria e revalidação deverá ser feita com base nas orientações fornecidas pela Fortinet na consultoria Incident Readiness.

6.2. A Contratada deverá configurar as seguintes soluções Fortinet

- FortiAuthenticator com licença SSO;
- FortiTokenMobile;
- FortiAnalyzer;
- FortiClient EMS com função de ZTNA;
- FortiEDR.

6.3. A Contratada será responsável por configurar por completo cada uma das soluções acima especificadas, sendo dado como aceito o funcionamento quando um total de 10% (dez) do total de licenças esteja plenamente em funcionamento. A Contratada deverá fazer um repasse de conhecimento para a equipe técnica da Contratante de modo que esta possa dar continuidade na implantação para os demais usuários/equipamentos.

6.4. A Contratada será responsável por configurar o FortiAuthenticator para validar os acessos dos usuários remotos que farão uso do FortiTokenMobile, ferramenta esta que ficará instalada em dispositivos móveis.

6.5. A Contratada será a responsável pela implantação do FortiAnalyzer e configuração / customização dos dispositivos fornecidos para o envio de logs para esta ferramenta de análise.

6.6. A Contratada será responsável por implantar o FortiClient EMS de modo que os usuários externos tenham uma segurança no acesso via esta ferramenta de confiança zero, a qual fará a validação de conformidade de dispositivos e usuários no acesso remoto.

6.7. A Contratada deverá criar templates, configurar servidores, máquinas e profiles do FortiEDR.

6.8. Deverá ser fornecido pela Contratada um treinamento de todas as soluções fornecidas, por um profissional com certificação mínima NSE7, com carga horária mínima de 24 (vinte e quatro) horas, para uma turma de até 6 (seis) pessoas.

6.9. O projeto deverá ser gerenciado por profissional Gerente de Projetos com certificação PMP do PMI ou com pós-graduação em Gerenciamento de Projetos.

6.10. O projeto deverá ser implantado por profissional com certificação mínima NSE7 do fabricante Fortinet.

6.11. A Contratada deverá considerar a participação presencial no projeto por no mínimo 5 (cinco) dias de um profissional com certificação Fortinet conjunto com o Gerente de Projetos para entendimento e consultoria inicial do ambiente envolvido neste projeto.

7. QUALIFICAÇÃO TÉCNICA

7.1. Comprovação de revendedor autorizado do fabricante da solução de segurança baseada em inteligência artificial.

8. ESPECIFICAÇÕES

8.1. Solução de centralização de logs

8.1.1. A solução deve ser baseada em máquina virtual do mesmo fabricante da solução de NGFW e SD-WAN e ter como objetivo a coleta, armazenamento e análise automatizada de registros em modo centralizado de todos os equipamentos a partir de uma única console de administração;

8.1.2. Deve ser do mesmo fabricante e totalmente compatível com os NG Firewalls implantados modelo Fortinet FortiGate permitindo a coleta de logs e a disponibilização de relatórios;

8.1.3. Deve acompanhar suporte ou subscrição por 36 meses.

8.1.4. Poderá ser entregue em formato appliance virtual;

8.1.5. Deverá estar devidamente licenciada para:

8.1.6. Suportar a coleta de, no mínimo, 50 GB de logs diários;

8.1.7. Caso a solução seja entregue como appliance virtual, este deve suportar:

8.1.8. Deve ser compatível com os hypervisor VMWare ESXi, Hyper-V e KVM;

8.1.9. Não deverá existir limite para o número de vCPUs no appliance virtual;

8.1.10. Não deverá existir limite para a expansão da memória RAM no appliance virtual;

8.1.11. Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual em nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;

8.1.12. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

8.1.13. Realizar o backup das configurações para permitir o retorno de uma configuração salva;

8.1.14. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;

8.1.15. Deve suportar a definição de perfis de acesso a console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

8.1.16. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

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

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

8.1.19. Utilizar técnicas de machine learning para a captura de índices de comprometimento, através de URLs, domínios e endereços IPs maliciosos;

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

8.1.21. Deve oferece um portal do cliente fácil de usar, permitindo acesso às capacidades seguras de SD-WAN, como monitoramento e modelos SD-WAN, políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação e links;

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

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

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

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

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

8.1.27. Deve possuir mecanismos de remoção automática para logs antigos;

8.1.28. Permitir importação e exportação de relatórios

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

8.1.30. Deve permitir exportar os logs no formato CSV;

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

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

8.1.33. A solução deve ter relatórios predefinidos;

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

8.1.35. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

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

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

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

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

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

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

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

8.1.43. Permitir o envio por e-mail relatórios automaticamente;

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

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

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

8.1.47. Deve permitir o uso de filtros nos relatórios;

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

8.1.49. Permitir especificar o idioma dos relatórios criados;

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

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

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

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

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

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

8.1.56. Deve permitir visualizar em tempo real os logs recebidos;

8.1.57. Deve permitir o encaminhamento de log no formato syslog;

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

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

8.1.60. Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados;

8.1.61. Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de "Zero Day" encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição;

8.1.62. Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo dela, tipos de indústria que já foram alvo do malware, comportamento malicioso conhecido sobre o malware e quais são os autores;

8.1.63. Deve permitir gerar alertas de eventos a partir de logs recebidos;

8.1.64. Deve suportar o serviço de Indicadores de Compromisso (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar pelo menos: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça), o número de ameaças detectadas;

8.1.65. A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato de 36 (trinta e seis) meses.

8.2. Solução de identificação e autenticação centralizada

8.2.1. A solução de ZTNA deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas;

8.2.2. Deve ser compatível e do mesmo fabricante da solução de firewall FortiGate 1100E implementada no datacenter;

8.2.3. Deve ser fornecido 5000 (cinco mil) licenças com suporte por 36 meses.

8.2.4. A solução de ZTNA deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust;

8.2.5. A solução de ZTNA deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão;

8.2.6. A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário;

8.2.7. Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem;

8.2.8. O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante;

8.2.9. Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits); Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022; Mac OS X: versões 13, 12, 11 e 10.15; Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior;

8.2.10. A solução de ZTNA deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel.

8.2.11. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3;

8.2.12. Tanto mediante agente ou sem o agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários;

8.2.13. A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único pelo agente e deverá ainda ser compartilhado com o proxy de acesso;

8.2.14. Deve ser possível revogar o certificado de um agente por meio da console central;

8.2.15. O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso;

8.2.16. No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão;

8.2.17. Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional;

8.2.18. A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido;

8.2.19. Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central;

8.2.20. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug;

8.2.21. Deve ser possível exportar os logs diretamente a nível de agente;

8.2.22. Deve ser possível exigir uma senha para desconectar o agente da console central;

8.2.23. Deve existir a possibilidade de restringir o usuário de realizar back up da configuração do agente;

8.2.24. Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central;

8.2.25. Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes. Deve ser possível ainda atribuir tags aos endpoints de acordo com o indíce de comprometimento detectado pela solução de consolidação de logs, desde que haja licenciamento instalado para tal;

8.2.26. Deve ser possível configurar o agente para usar Proxy;

8.2.27. O agente deve permitir a configuração local via XML (eXtensible Markup Language);

8.2.28. Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;

8.2.29. Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML;

8.2.30. Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente;

8.2.31. Deve ser possível especificar a validade do código de registro;

8.2.32. A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net.

8.2.33. A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4;

8.2.34. Deve ser possível agrupar agentes em grupos;

8.2.35. Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;

8.2.36. Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política;

8.2.37. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão do agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA;

8.2.38. O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S;

8.2.39. Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, baseado no host field do cabeçalho HTTP ou baseado em disponibilidade do servidor;

8.2.40. Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor. Deste modo, o agente deve manipular o host file do endpoint visando criar entradas DNS;

8.2.41. Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;

8.2.42. A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa;

8.2.43. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;

8.2.44. As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da solução de ZTNA visando controlar a postura de um determinado endpoint diretamente no proxy de acesso;

8.2.45. A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas;

8.2.46. Deve ser possível construir tags com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas;

8.2.47. A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON;

8.2.48. Deve ser possível verificar quais endpoints estão associadas com cada tag;

8.2.49. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma tag simultaneamente, caso a política possua vínculo com diversas tags;

8.2.50. Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário;

8.2.51. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local;

8.2.52. Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais;

8.2.53. Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn, Google ou Salesforce, podendo ainda notificá-los para que esse vínculo possa ser realizado;

8.2.54. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades em nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança em nível de sistema operacional;

8.2.55. Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows;

8.2.56. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;

8.2.57. Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;

8.2.58. Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance;

8.2.59. Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático;

8.2.60. O agente deve dispor de um sistema de notificação do tipo pop-up visando alertar o usuário;

8.2.61. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente;

8.2.62. Deve suportar a criação de várias versões de pacotes de instalação;

8.2.63. As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software;

8.2.64. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente;

8.2.65. Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado;

8.2.66. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet;

8.2.67. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar;

8.2.68. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge;

8.2.69. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;

8.2.70. Deve ser possível determinar quando o filtro web entrará em ação no agente, se ele deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;

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

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

8.2.73. Deve acompanhar subscrição do serviço em nuvem e suporte pelo período de 36 (trinta e seis) meses.

8.3. Token para MFA

8.3.1. Deve ser fornecido para a 5000 (cinco mil) usuários;

8.3.2. Deve ser do tipo mobile e suportar autenticação em dois fatores através do aplicativo (iOS, Android e Windows);

8.3.3. Deve ser perpétuo;

8.3.4. Deve ser do mesmo fabricante e compatível com o firewall Fortinet Fortigate implementado no datacenter;

8.3.5. Deve oferecer proteção contra ataques do tipo “brute-force”;

8.3.6. Deve permitir a visualização do número de série no aplicativo;

8.3.7. Deve suportar OATH e OTP.

8.4. Solução de autenticação centralizada

8.4.1. Deve possuir licenciamento para 5000 (cinco mil) usuários locais ou remotos com suporte por 36 meses.

8.4.2. Deve incluir todos os recursos e licenciamento para funcionar em alta disponibilidade (ao menos 2 instâncias);

8.4.3. Deve ser do mesmo fabricante e compatível com o firewall Fortinet Fortigate implementado no datacenter;

8.4.4. Deve suportar administração em interface gráfica (GUI) por HTTP e/ou HTTPS;

8.4.5. Deve suportar administração em interface baseada em linhas de comando (CLI) por TELNET e/ou SSH;

8.4.6. Deve permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas;

8.4.7. Deve possuir Indicador visual, centralizado, de informações críticas (estado da licença, versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados);

8.4.8. Deve suportar a atualização do firmware via interface gráfica, por processo simplificado e intuitivo;

8.4.9. Deve suportar customização de mensagens padrão da solução como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas mensagens/páginas sem a necessidade de recursos ou conectividade externa;

8.4.10. Deve suportar configuração de Alta Disponibilidade (HA), reduzindo ao máximo os períodos de interrupção;

8.4.11. Deve suportar implementações de HA como "Ativo-Passivo" ou sincronizando configurações entre duas caixas ativas;

8.4.12. Deve permitir sincronismo automático de configurações entre todos os equipamentos que componham a solução em HA;

8.4.13. Deve suportar implementação de HA sincronizando configurações com appliances em localidades geograficamente separadas;

8.4.14. Deve suportar a opção de backup criptografado;

8.4.15. Deve suportar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;

8.4.16. Deve suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single-sign-on. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica;

8.4.17. Deve suportar NTP (Network Time Protocol), visando o sincronismo de hora/data;

8.4.18. Deve suportar SNMP v1, v2 e v3 permitindo consultar MIB própria e envio de Traps;

8.4.19. Deve suportar nativamente Trap SNMP indicando mudança de status de HA;

8.4.20. Deve suportar captura de pacotes através da interface gráfica para Troubleshoot avançado em ferramentas de análise de pacotes (ex.: Wireshark);

8.4.21. O equipamento deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, auto-registro de usuários e autenticação de segundo fator (token);

8.4.22. Deve suportar o registro de todos os eventos que os usuários de sua base de dados local realizem com suas contas, tais como criação de um usuário, troca de senha de um usuário e alteração de informação gerais;

8.4.22.1. AUTENTICAÇÃO

8.4.22.1.1. A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração dos mesmos sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados;

8.4.22.1.2. Deve suportar autenticação em dois fatores (two-factor authentication);

8.4.22.1.3. Deve possuir suporte a autenticação de dois fatores em pelo menos dois tipos diferentes de tokens, sendo o primeiro físico (token), e o segundo lógico como software para dispositivos móveis, e-mail ou SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário. Tokens e licenciamento de SMS não inclusos nesta especificação;

8.4.22.1.4. Deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais e etc;

8.4.22.1.5. Deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta;

8.4.22.1.6. Deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;

8.4.22.1.7. Deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos;

8.4.22.1.8. Deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação;

8.4.22.1.9. Deve permitir a criação de novos usuários na base de dados local de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário;

8.4.22.1.10. Deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que o mesmo utilize o token como único fator de autenticação;

8.4.22.1.11. Deve permitir associar os tokens aos usuários criados localmente na base de dados;

8.4.22.1.12. Deve permitir que os próprios usuários façam o registro dos seus tokens e relatem a perda de um token automaticamente, sem necessidade de envolver um administrador;

8.4.22.1.13. Deve permitir remoção automática em massa de usuários desabilitados, baseado em critérios definidos;

8.4.22.1.14. Deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança;

8.4.22.1.15. Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;

8.4.22.1.16. Os tokens devem gerar códigos com no mínimo 6 dígitos e intervalos não superiores à 60 segundos;

8.4.22.1.17. Deve suportar autenticação em dois fatores por hardware dedicado (Token);

8.4.22.1.18. Deve suportar autenticação em dois fatores por aplicativo mobile (iOS e Android);

8.4.22.1.19. Deve suportar autenticação em dois fatores por envio de e-mail;

8.4.22.1.20. Deve suportar a sincronização com dispositivo em hardware de geração de OTP (One Time Password);

8.4.22.1.21. Deve permitir sincronizar os tokens com o equipamento para o correto funcionamento dos mesmos.

8.4.22.1.22. Deve permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado;

8.4.22.1.23. Deve permitir a desassociação de um token a um usuário e associá-lo a outro usuário quando necessário, permitindo assim que sejam reaproveitados;

8.4.22.1.24. Deve continuar permitindo a autenticação de dois fatores em clientes windows mesmo com a máquina offline;

8.4.22.1.25. Deve prover um portal web para o auto-registro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro,

o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado;

8.4.22.1.26. Deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;

8.4.22.1.27. Deve suportar a integração com servidor RADIUS remoto;

8.4.22.1.28. Deve ter capacidade de funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;

8.4.22.1.29. Deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory);

8.4.22.1.30. Deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;

8.4.22.1.31. Deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;

8.4.22.1.32. Deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;

8.4.22.1.33. Deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes;

8.4.22.1.34. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo uma relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);

8.4.22.1.35. Deve permitir integração com bases do Azure Directory e Gsuite;

8.4.22.1.36. Por meio do SAML, deve permitir integrações com SPs variados, tais como Office 365;

8.4.23. CERTIFICADOS

8.4.23.1. Deve atuar como Autoridade Certificadora (CA);

8.4.23.2. Deve permitir a administração de certificados digitais, com emissão e revogação;

8.4.23.3. Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas;

8.4.23.4. Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL);

8.4.23.5. Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados;

8.4.23.6. Deve suportar SCEP Server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador;

8.4.23.7. Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados;

8.4.23.8. Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários;

8.4.24. SERVIÇO DE AUTENTICAÇÃO ÚNICA (SINGLE SIGN-ON)

8.4.24.1. Deve prover capacidade de serviço SSO (Single Sign-On), com autenticação transparente (passiva) de usuários em sistemas compatíveis;

8.4.24.2. Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade se SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio;

8.4.24.3. Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO;

8.4.24.4. Deve suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO;

8.4.24.5. Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros;

8.4.24.6. Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On);

8.4.24.7. Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accouting, a modificação destes pacotes e o encaminhamento deles para vários outros pontos.

8.4.25. Solução de proteção para endpoint

8.4.25.1. A solução de ZTNA deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas.

8.4.25.2. Deve ser compatível com o firewall Fortinet FortiGate, permitindo o aproveitamento da base instalada e menor complexidade para os recursos de ZTNA.

8.4.25.3. Deve ser fornecido para 5000 (cinco mil) usuários com suporte por 36 meses.

8.4.25.4. A solução de ZTNA deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust.

8.4.25.5. A solução de ZTNA deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão.

8.4.25.6. A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por usuário.

8.4.25.7. Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem.

8.4.25.8. O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante.

8.4.25.9. A solução de ZTNA deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel.

8.4.25.10. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3.

8.4.25.11. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.

8.4.25.12. A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.

8.4.25.13. Deve ser possível revogar o certificado de um agente por meio da console central.

8.4.25.14. O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso.

8.4.25.15. No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão.

8.4.25.16. Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional.

8.4.25.17. A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido.

8.4.25.18. Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central.

8.4.25.19. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug.

8.4.25.20. Deve ser possível exportar os logs diretamente a nível de agente.

8.4.25.21. Deve ser possível exigir uma senha para desconectar o agente da console central.

8.4.25.22. Deve existir a possibilidade de restringir o usuário de realizar back up da configuração do agente.

8.4.25.23. Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central.

8.4.25.24. Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes. Deve ser possível ainda atribuir tags aos endpoints de acordo com o indíce de comprometimento detectado pela solução de consolidação de logs, desde que haja licenciamento instalado para tal.

8.4.25.25. Deve ser possível configurar o agente para usar Proxy.

8.4.25.26. O agente deve permitir a configuração local via XML (eXtensible Markup Language);

8.4.25.27. Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central.

8.4.25.28. Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML.

8.4.25.29. Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente.

8.4.25.30. Deve ser possível especificar a validade do código de registro.

8.4.25.31. A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net.

8.4.25.32. A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4.

8.4.25.33. Deve ser possível agrupar agentes em grupos.

8.4.25.34. Deve ser possível atribuir grupos de agentes a perfis de políticas específicos.

8.4.25.35. Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política.

8.4.25.36. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA.

8.4.25.37. O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S.

8.4.25.38. Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, baseado no host field do cabeçalho HTTP ou baseado em disponibilidade do servidor.

8.4.25.39. Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor. Deste modo, o agente deve manipular o host file do endpoint visando criar entradas DNS.

8.4.25.40. Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas.

8.4.25.41. A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa.

8.4.25.42. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas.

8.4.25.43. As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da solução de ZTNA visando controlar a postura de um determinado endpoint diretamente no proxy de acesso.

8.4.25.44. A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas.

8.4.25.45. Deve ser possível construir tags com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas.

8.4.25.46. A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON.

8.4.25.47. Deve ser possível verificar quais endpoints estão associadas com cada tag.

8.4.25.48. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma tag simultaneamente, caso a política possua vínculo com diversas tags.

8.4.25.49. Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário.

8.4.25.50. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local.

8.4.25.51. Deve possibilitar definir funções administrativas realcionadas às permissões dos endpoints, de políticas e de configurações gerais.

8.4.25.52. Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn, Google ou Salesforce, podendo ainda notificá-los para que esse vínculo possa ser realizado.

8.4.25.53. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional.

8.4.25.54. Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows.

8.4.25.55. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente.

8.4.25.56. Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos.

8.4.25.57. Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance.

8.4.25.58. Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático.

8.4.25.59. O agente deve dispor de um sistema de notificação do tipo popup visando alertar o usuário.

8.4.25.60. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente.

8.4.25.61. Deve suportar a criação de várias versões de pacotes de instalação.

8.4.25.62. As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software.

8.4.25.63. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente.

8.4.25.64. Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser

possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado.

8.4.25.65. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet.

8.4.25.66. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar.

8.4.25.67. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge.

8.4.25.68. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário.

8.4.25.69. Deve ser possível determinar quando o filtro web entrará em ação no agente, se ele deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa.

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

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

8.4.25.72. Deve incluir funcionalidades de antivírus, englobando, no mínimo:

8.4.25.72.1. Antivírus com recursos de inteligência artificial para detecção;

8.4.25.72.2. Controle de dispositivos removíveis (pen drive);

8.4.25.72.3. Quarentena automatizada;

8.4.25.72.4. Firewall de aplicações instaladas no sistema;

8.4.25.72.5. Proteção contra ransonware.

8.5. Solução de proteção e resposta à incidente

8.5.1. Deve suportar integração nativa com o firewall FortiGate onde um controle de ZTNA (Zero Trust Network Access) possa ser amplamente estabelecido por intermédio de verificação de postura do endpoint, de forma que, ao identificar um processo potencialmente malicioso no endpoint alvo, a solução possa enviar informações de restrição/bloqueio ao FortiGate e/ou

componentes de Zero Trust para tomada de ação automatizada, a fim de não permitir o acesso desse ativo a aplicações e sistemas críticos a partir da máquina com suspeita ou até mesmo comprometida. As regras de bloqueio e restrição deverão ser necessariamente configuráveis, permitindo que o acesso possa restringido por aplicação e/ou de forma granular por regras de firewall a ser definido administrativamente pela prefeitura, sem a necessidade da criação de scripts por parte da prefeitura para realizar as integrações.

8.5.2. Deve ser possível integrar-se a arquitetura de Zero Trust (ZTNA), a validação da instalação do agente de EDR dentro do dispositivo dos usuários e servidores, de modo a conseguir definir que apenas dispositivos com postura validada e que possuam a solução de EDR previamente instalada no endpoint alvo possam ter seus acessos permitidos pelas políticas de ZTNA do firewall de rede em questão (Fortinet Fortigate).

8.5.3. Deve ser fornecido para 5000 (cinco mil) usuários com suporte por 36 meses.

8.5.4. A solução proposta deve ser compatível com os seguintes sistemas operacionais: Windows (versões 32 e 64 bits) XP SP2 / SP3, 7, 8, 8.1 e 10.

8.5.5. A solução proposta deve ser compatível com os seguintes sistemas operacionais: Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 e 2019.

8.5.6. A solução proposta deve ser compatível com os seguintes sistemas operacionais: versões macOS: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) e Catalina (10.15)

8.5.7. A solução proposta deve ser compatível com os seguintes sistemas operacionais: Versões do Linux: RedHat Enterprise Linux e CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 e 7.7 e Ubuntu LTS 16.04.5, 16.04.6, 6.8. § servidor 18.04.1 e 18.04.2, 64 bits".

8.5.8. A solução proposta deve ser compatível com os seguintes sistemas operacionais: Ambientes de Virtual Desktop Infrastructure (VDI) em VMware E Citrix. VMware Horizons 6 e 7 e Citrix XenDesktop 7.

8.5.9. A solução proposta deve ser compatível com os seguintes sistemas operacionais: Oracle Linux OL (antigo OEL).

8.5.10. A solução proposta deve ter um consumo máximo de 120 MB de memória RAM.

8.5.11. A solução proposta deve ter um consumo médio de menos de 2% do uso da CPU.

8.5.12. A solução proposta deve consumir menos de 20 MB de espaço em disco.

8.5.13. A solução proposta deve oferecer suporte à implantação em massa por meio de ferramentas como MS System Center, JAMF e Satellite.

8.5.14. A solução proposta deve ter a capacidade de atualizar o terminal sem interação do usuário e sem exigir uma reinicialização.

8.5.15. A solução proposta deve ter proteção "Anti-violação" no Agente.

8.5.16. A solução proposta deve funcionar sem depender de assinaturas hash locais conhecidas para a detecção de arquivos maliciosos.

8.5.17. A solução proposta deve ser capaz de registrar em tempo real informações do processo e informações adicionais, como o conhecimento do usuário associado aos eventos.

8.5.18. A solução proposta deve ter a opção de definir a senha para desinstalar o agente no terminal.

8.5.19. A solução proposta deve ser capaz de gerar um instalador Windows pré-configurado. Esta configuração deve permitir a instalação sem a necessidade de interação ou configuração do usuário.

8.5.20. O coletor que será instalado nos terminais da solução proposta deve ser capaz de trabalhar por trás de um proxy.

8.5.21. DETECÇÃO

8.5.22. A solução proposta deve ser capaz de funcionar no modo "offline" sem que o Agente esteja conectado à rede corporativa.

8.5.23. A solução proposta deve ser capaz de detectar processos em execução, inícios de processos, paradas de processos e interações entre processos.

8.5.24. A solução proposta deve ser capaz de detectar, eliminar e retornar ao seu valor inicial as alterações feitas por processos maliciosos no registro do PC.

8.5.25. A solução proposta deve ser capaz de detectar as solicitações de DNS enviadas do dispositivo.

8.5.26. A solução proposta deve ser capaz de detectar conexões de rede a partir do dispositivo.

8.5.27. A solução proposta deve ser capaz de detectar atividades suspeitas associadas a arquivos DLL.

8.5.28. A solução proposta deve ser capaz de incorporar inteligência de ameaças ao esquema de detecção.

8.5.29. A solução proposta deve ser capaz de incorporar as técnicas MITER ATT&CK no esquema de detecção e mostrar quais dessas técnicas foram utilizadas.

8.5.30. A solução proposta deve ter a capacidade de pesquisar ameaças nas estações do Windows usando indicadores de comprometimento (IOC), como: nome do arquivo e hash do arquivo, etc.

8.5.31. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas a arquivos (Criação, Exclusão, Renomear).

8.5.32. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas a processos (Terminação de Processo, Criação de Processo, Carregamento de Executáveis).

8.5.33. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao uso da rede (Socket Connect, Socket Close, Socket Brind).

8.5.34. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas aos logs do Windows (Log de eventos).

8.5.35. A solução proposta deve ter a capacidade de pesquisar ameaças nas estações do Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao registro do Windows (criação de chave, exclusão de chave, conjunto de valores).

8.5.36. A solução proposta deve ter a capacidade de realizar consultas de texto livre para filtrar as informações disponíveis para a caça de ameaças.

8.5.37. A solução proposta deve ter a capacidade de armazenar pesquisas realizadas para serem reutilizadas no futuro.

8.5.38. A solução proposta deve ter a capacidade de agendar pesquisas armazenadas.

8.5.39. A solução proposta deve identificar atividades maliciosas conhecidas.

8.5.40. A solução proposta deve ter a capacidade de receber atualizações diárias de inteligência.

8.5.41. A solução proposta deve ter a capacidade de categorizar os eventos detectados em diferentes categorias (Ex: Malicioso, Suspeito, Inconclusivo, Provavelmente Seguro).

8.5.42. A solução proposta deve ter a capacidade de coexistir com outras soluções de segurança de endpoint do tipo de antivírus tradicional ou de nova geração.

8.5.43. PREVENÇÃO

8.5.43.1. A solução proposta deve ter a capacidade de prevenir a execução de arquivos maliciosos.

8.5.43.2. A solução proposta deve incorporar um mecanismo de antivírus de última geração (Next-Generation Antivírus) baseado no kernel do sistema operacional, com capacidade de "Aprendizado de Máquina" (Machine Learning).

8.5.43.3. A solução proposta deve ter a capacidade de controlar dispositivos USB.

8.5.43.4. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no nome do dispositivo.

8.5.43.5. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no fornecedor do dispositivo.

8.5.43.6. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no número de série do dispositivo.

8.5.43.7. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base em uma combinação de: nome do dispositivo, fornecedor, número de série.

8.5.43.8. A solução proposta deve ser capaz de bloquear o tráfego malicioso de exfiltração de dados.

8.5.43.9. A solução proposta deve ser capaz de bloquear o tráfego de comunicação malicioso para C&C (Comando e Controle).

8.5.43.10. A solução proposta deve ser capaz de impedir violações de segurança e tentativas de ransomware em tempo real.

8.5.43.11. A solução proposta deve ser capaz de evitar a criptografia causada por ransomware e modificação de arquivos ou registro de dispositivos, caso isso ocorra, a solução deverá restaurar os arquivos afetados/modificados para o seu estado original em tempo real.

8.5.43.12. A solução proposta deve permitir que as políticas nela contidas sejam modificadas permitindo vários estados tais como: Ativo, Desativado ou apenas criar "logs" para as regras de segurança contidas nestes.

8.5.43.13. A solução proposta deve ser capaz de ser configurada em modo de simulação onde nenhum bloqueio é feito, mas todas as atividades maliciosas são registradas.

8.5.43.14. A solução proposta deve ser capaz de permitir a modificação das regras de detecção de eventos maliciosos de forma que essas regras apenas armazenem um registro ou fiquem em modo de bloqueio.

8.5.43.15. A solução proposta deve ser capaz de permitir verificações periódicas dos arquivos contidos nos dispositivos com o Agente instalado.

8.5.44. PÓS INFECÇÃO

8.5.44.1. A solução proposta deve permitir o isolamento automático do tráfego de rede de um dispositivo onde foi encontrada uma atividade causada por malware.

8.5.44.2. A solução proposta deve permitir alterar as políticas atribuídas de um dispositivo onde uma atividade causada por malware foi encontrada.

8.5.44.3. A solução proposta deve permitir o bloqueio de atividades realizadas por arquivos maliciosos.

8.5.44.4. A solução proposta deve ter a capacidade de criar exceções para processos com base na localização do arquivo (Caminho do Arquivo).

8.5.44.5. A solução proposta deve ter a capacidade de criar exceções para processos com base no destino do tráfego gerado pelo processo.

8.5.44.6. A solução proposta deve ter a capacidade de criar exceções para os processos baseados no usuário que o processo executou.

8.5.44.7. A solução proposta deve ter a capacidade de criar exceções manualmente para falsos positivos para marcar a atividade como um falso positivo e evitar a ocorrência de falhas futuras.

8.5.44.8. A solução proposta deve ter a capacidade de reclassificar automaticamente a atividade como um falso positivo e evitar a ocorrência de detecções semelhantes.

8.5.44.9. A solução proposta deve permitir a criação de exceções de eventos com base em endereços IP, aplicações e protocolos.

8.5.45. RESPOSTA AO INCIDENTE

8.5.45.1. A solução proposta deve permitir um histórico dos eventos por no mínimo 6 meses.

8.5.45.2. A solução proposta deve armazenar metadados gerados pelos dispositivos para que possam ser usados em investigações forenses.

8.5.45.3. A solução proposta deve permitir a integração com plataformas SIEMs (Security Information and Event Management) através de um syslog.

8.5.45.4. A solução proposta deve ter a capacidade de obter instantâneos de memória ou "dumps" de memória que permitam a realização de processos forenses.

8.5.45.5. A solução proposta deve ter a capacidade de abrir tickets em plataformas de gerenciamento como ServiceNow e JIRA.

8.5.45.6. A solução proposta deve permitir a integração através de API onde tem a capacidade de entregar informações geradas em um evento como: endereço IP, nome do host, usuário, data / hora ocorrida, atividade suspeita, etc.) para permitir a integração via API.

8.5.45.7. A solução proposta deve ter a capacidade de encerrar um processo com base em sua classificação.

8.5.45.8. A solução proposta deve ter a capacidade de excluir um arquivo com base em sua classificação.

8.5.45.9. A solução proposta deve ser a capacidade de restaurar as configurações de registro básicas com base na classificação de atividade predefinida.

8.5.45.10. A solução proposta deve ter a capacidade de isolar os dispositivos infectados da rede.

8.5.45.11. A solução proposta deve ter a capacidade de restringir automaticamente o acesso do dispositivo à rede de acordo com a classificação (Malicioso, Suspeito, etc.) do processo detectado.

8.5.45.12. A solução proposta deve obter visibilidade total da cadeia de ataques e alterações maliciosas.

8.5.45.13. A solução proposta deve permitir a limpeza automática do dispositivo e reverter alterações maliciosas, mantendo o tempo de atividade do dispositivo.

8.5.45.14. A solução proposta deve permitir a assinatura de serviços opcionais de detecção e resposta a incidentes (Ex: serviços gerenciados de detecção e resposta).

8.5.45.15. A solução proposta deve permitir o envio de executáveis para análise em um sandbox, a fim de determinar se são maliciosos ou inofensivos.

8.5.45.16. A solução proposta deve possuir integração com Active Directory a fim de possibilitar a utilização de playbooks para contenção e resposta à incidentes de segurança.

8.5.45.17. A solução proposta deve fornecer vários mecanismos de proteção, incluindo o encerramento de um processo, a exclusão de um arquivo malicioso, o bloqueio de uma conexão de rede.

8.5.46. CONTROLE DE VULNERABILIDADES

8.5.46.1. A solução proposta deve ter a capacidade de descobrir aplicativos que estão se comunicando através da rede e que representam risco para o terminal.

8.5.46.2. A solução proposta deve ter capacidade para realizar um patch virtual, através da restrição de acessos de comunicação nas aplicações vulneráveis.

8.5.46.3. A solução proposta deve permitir a redução das superfícies de ataque utilizando políticas de comunicação proativas baseadas no risco de acordo com o CVE e a qualificação ou reputação que uma aplicação possa ter.

8.5.46.4. A solução proposta deve ter a capacidade de impedir que aplicativos não autorizados se comuniquem pela rede.

8.5.46.5. A solução proposta deve ter a capacidade de criar políticas que tenham a capacidade de impedir a comunicação de aplicativos de acordo com a versão do aplicativo instalado.

8.5.46.6. A solução proposta deve ser capaz de detectar e identificar todas as aplicações nos dispositivos que se comunicam na rede.

8.5.46.7. A solução proposta deve ser capaz de fornecer informações sobre o uso de aplicativos de rede mostrando, por exemplo, quais dispositivos geram tráfego para um aplicativo.

8.5.46.8. A solução proposta deve ser capaz de visualizar e entregar informações sobre o uso dos aplicativos de rede mostrando informações como os destinos IP do tráfego gerado pelo aplicativo.

8.5.47. CENÁRIOS DE ATAQUE

8.5.47.1. A solução proposta deve identificar e prevenir tentativas de perseguição de privilégios.

8.5.47.2. A solução proposta deve bloquear ataques de ransomware conhecidos.

8.5.47.3. A solução proposta deve detectar malware desconhecido como RAT (Trojan de acesso remoto) por meio das atividades do malware e não de uma assinatura.

8.5.47.4. A solução proposta deve proteger contra scripts Powershell maliciosos.

8.5.47.5. A solução proposta deve proteger contra scripts CScript maliciosos.

8.5.47.6. A solução proposta deve proteger contra macros maliciosas do Office.

8.5.47.7. A solução proposta deve ter controle sobre dispositivos USB.

8.5.48. INTERNET DAS COISAS (IOT)

8.5.48.1. A solução proposta deve ter a capacidade de descobrir dispositivos IOT não gerenciados na rede.

8.5.48.2. A solução proposta deve ter a capacidade de detectar dispositivos não gerenciados e protegidos pela solução com sistemas operacionais macOS / Linux / Windows.

8.5.49. ADMINISTRAÇÃO

8.5.49.1. A Solução deve conter políticas de segurança e playbooks básicos pré-definidos, sem que haja a necessidade de criação manual logo após a instalação da solução.

8.5.49.2. A solução proposta deve estar em conformidade com o padrão GDPR.

8.5.49.3. O console de gerenciamento da solução proposta deve permitir a integração com o "Active Directory" para garantir o cumprimento dos requisitos da política de senhas da empresa.

8.5.49.4. O console de administração da solução proposta deve permitir o uso de autenticação de dois fatores (2FA) para acessá-la.

8.5.49.5. O console de administração da solução proposta deve permitir a integração com SAML para autenticação do usuário no console de gerenciamento.

8.5.49.6. O console de administração da solução proposta deve permitir o uso de funções granulares para administradores.

8.5.49.7. O console de administração da solução proposta deve permitir o gerenciamento de ambientes multilocatários.

8.5.49.8. O console de administração da solução proposta deve permitir o gerenciamento por meio da API Full Restful.

8.5.49.9. A solução proposta deve ser capaz de ser totalmente gerenciada na nuvem sem a necessidade de serviços locais.

8.5.49.10. A solução proposta deve ser capaz de ser gerenciada em uma arquitetura híbrida usando serviços locais complementados com outros na nuvem.

8.5.49.11. A solução proposta deve permitir integração com Fortinet FortiGate existente no ambiente.

8.5.49.12. O console de administração da solução proposta deve permitir a visualização dos eventos registrados nos dispositivos que requerem atenção.

8.5.49.13. O console de administração da solução proposta deve permitir a visualização da saúde dos Agentes instalados.

8.5.49.14. O console de administração da solução proposta deve permitir a desinstalação remota do Agente instalado nos dispositivos.

8.5.49.15. O console de administração da solução proposta deve permitir a desativação / ativação remota do Agente instalado nos dispositivos.

8.5.49.16. O console de administração da solução proposta deve permitir a atualização remota do Agente instalado nos dispositivos.

8.5.49.17. O console de administração da solução proposta deve permitir a criação de relatórios executivos contendo um resumo que descreva os eventos de segurança e o status do sistema.

8.5.49.18. O console de administração da solução proposta deve permitir a criação de grupos organizacionais de dispositivos nos quais cada grupo possa ter regras de proteção independentes dos demais.

8.5.49.19. O console de administração da solução proposta deve permitir a exportação dos logs locais gerados pelos Agentes a partir do mesmo console.

8.5.49.20. O console de administração da solução proposta deve permitir a criação de relatórios de inventário dos Agentes implantados contendo informações como: Endereço IP, Nome do Host, Sistema Operacional, Endereço MAC, Versão do Agente instalado, Status do Agente, Último dia visto pelo console.

8.5.49.21. O console de gerenciamento da solução proposta deve ter a visibilidade dos eventos gerados pelos dispositivos ou eventos de acordo com o processo executado.

8.5.49.22. O console de administração da solução proposta deve permitir a integração de um SMTP externo para envio de alertas por e-mail.

8.5.49.23. O console de administração da solução proposta deve permitir auditorias de alterações feitas por administradores / operadores. Essas auditorias também devem ser baixadas em formato CSV.

8.5.49.24. A solução proposta deve exigir que uma senha seja desabilitada por um aplicativo de terceiros.

8.5.49.25. A solução proposta deve permitir o isolamento de um dispositivo através da integração de um NAC de acordo com a categoria do evento detectado.

8.5.49.26. A solução proposta deve permitir adicionar endereços IP maliciosos detectados em um ou mais firewalls remotos integrados.

8.5.49.27. A solução proposta deve permitir a configuração de perfis nas informações coletadas para a função de caça a ameaças.

8.5.49.28. A solução proposta deve permitir exclusões de informações que não serão coletadas na função de caça a ameaças.

8.5.49.29. A solução proposta deve ser certificada pela Microsoft como uma solução antivírus e ser capaz de se integrar com o Windows Security Center.

8.5.49.30. A solução proposta deve entregar informações geradas pelos serviços de inteligência para a tomada de decisão na nuvem sobre o evento detectado.

8.5.49.31. A solução proposta deve permitir que os serviços em nuvem recategorizem uma classificação de evento.

8.5.49.32. A solução proposta deve permitir que os administradores desabilitem as notificações para um evento de descoberta.

8.5.49.33. A solução proposta deve permitir que as funções de filtragem da web sejam realizadas bloqueando o acesso às páginas da web categorizadas como maliciosas.

9. Serviço de resposta à incidente

9.1. Com o intuito de investigar o ambiente existente, a identificou-se a necessidade de contratação de um serviço de análise forense para avaliar as condições do ambiente existente. O objetivo é identificar se o atacante ainda tem acesso ao ambiente, efetuar a correção da falha e implementar as novas ferramentas.

9.2. Avaliação de comprometimento e riscos;

9.3. Apoio na definição do processo de resposta ao incidente;

9.4. Serviço de “threat huting”;

9.5. SLA inferior a 4 horas para tratamento de incidentes;

9.6. O serviço deve ser executado por 12 meses;

9.7. O serviço deve ser executado pelo fabricante da solução proposta no item 1;

9.8. O serviço deve ser especializado no atendimento de ransonware;

9.9. Deve utilizar a solução de EDR do mesmo fabricante para apoiar na detecção;

Sabrina Medianeira da Silva Avila
Analista de Sistemas

Tiago Martini Sanchotene
Secretário de Inovação e Tecnologia da Informação

ANEXO III

PREGÃO ELETRÔNICO Nº 170/2023

MODELO DE PROPOSTA FINANCEIRA

Empresa:
Endereço:
CNPJ:
Fone/e-mail:

lote	item	Unidade	Cód prod.	Descrição	Comp.	Quant	Marca	Valor Unitário	Valor Total
1	**1**	**SV**	**39622**	**SOLUÇÃO XDR BASEADO EM INTELIGÊNCIA ARTIFICIAL COM INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE – CONFORME TERMO DE REFERÊNCIA**		**5.000**			
1	**2**	**SV**	**34566**	SERVIÇOS TÉCNICOS ESPECIALIZADOS, CONFORME TERMO DE REFERÊNCIA	**Assistência especializada a incidentes (12 meses)**	**1**			

a) Declaramos que concordamos integralmente com as condições estipuladas na presente licitação e, que se vencedor deste certame, nos submeteremos ao cumprimento de seus termos.

b) A validade da proposta é de 60 (sessenta) dias corridos, contados da data de recebimento das propostas, conforme estipulado no Edital.

Local, ____de _____de 2023.

_____

Nome e Assinatura (Representante Legal)

CPF

RG

ANEXO IV

PREGÃO ELETRÔNICO Nº 170/2023

PREÇO MÁXIMO ESTIMADO

Item	D E S C R I Ç Ã O	Comp.	Quant.	Valor unitário	Preço médio orçado
1	SOLUÇÃO XDR BASEADO EM INTELIGÊNCIA ARTIFICIAL COM INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE – CONFORME TERMO DE REFERÊNCIA		5.000	633,6000	3.168.000,00
2	SERVIÇOS TÉCNICOS ESPECIALIZADOS, CONFORME TERMO DE REFERÊNCIA	Assistência especializada a incidentes (12 meses)	1	2.112.000,0000	2.112.000,00

ANEXO V

PREGÃO ELETRÔNICO Nº 170/2023

PROCESSO Nº 709/2023

MINUTA DE CONTRATO DE PRESTAÇÃO DE SERVIÇO

CONTRATO PARA **CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO COM INSTALAÇÃO SUPORTE E SERVIÇO DE RESPOSTA A INCIDENTES (SOLUÇÃO XDR)** QUE CELEBRAM ENTRE SÍ, O MUNICÍPIO DE SANTA MARIA E A EMPRESA _____, CONFORME LICITAÇÃO, REGISTRADA NA MODALIDADE PREGÃO ELETRÔNICO, SOB O N.º 170/2023, HOMOLOGADA EM __ DE _____ DE 2023.

PREÂMBULO

O Município de Santa Maria, inscrito no Cadastro Nacional da Pessoa Jurídica – CNPJ, sob o número 88.488.366/0001-00, estabelecido à Rua Venâncio Aires, n.° 2277, nesta cidade, representado neste ato pelo seu Prefeito Municipal, o Sr. Jorge Cladistone Pozzobom, doravante denominado CONTRATANTE, e de outro lado a empresa _____, inscrita no CNPJ/MF sob o n.º _____, doravante denominada CONTRATADA, neste ato representada pelo Sr. _____, inscrito no Registro Geral sob o n.º _____ e no Cadastro de Pessoas Físicas sob o n.º _____', resolvem celebrar o presente contrato para a execução do objeto descrito na Cláusula Primeira, em conformidade com Lei Federal de Licitações n.º 8666/93, Lei Federal n.º 10.520/2002, Decreto Municipal n.º 072/2015, de 03 de agosto de 2015, bem como de acordo com as cláusulas e condições que abaixo seguem expostas:

CLÁUSULA PRIMEIRA - DO OBJETO

O presente contrato tem por objeto **Contratação de Solução de Segurança da Informação com instalação suporte e serviço de resposta a incidentes (Solução XDR)** do Edital de Licitação, e de acordo com o exposto a seguir:

PARÁGRAFO ÚNICO – O objeto deste contrato deverá estar de acordo com as condições e características contidas no Processo Licitatório n.º 709/2023, Pregão Eletrônico n.º 170/2023 e seus anexos, Empenho n.º _____/2023, com a proposta da CONTRATADA, com a legislação vigente, com as cláusulas deste instrumento contratual e demais legislação pertinente.

CLÁUSULA SEGUNDA - DO PREÇO

O preço total para a execução do objeto deste Contrato é de **R$** _____ (mil reais), sendo o valor entendido este, como justo e suficiente para a total execução do especificado na Cláusula Primeira deste instrumento contratual.

CLÁUSULA TERCEIRA – DA EXECUÇÃO DOS SERVIÇOS

§1.º Vigência:

Para o item 1: o prazo de vigência do contrato será de 36 (trinta e seis) meses consecutivos e ininterruptos, a partir de sua assinatura, podendo o mesmo ser prorrogado por igual período ou rescindido, conforme interesse público, de acordo com a Lei Federal nº 8.666/93 e suas posteriores alterações.

Para o item 2: o prazo de vigência do contrato será de 12 (doze) meses consecutivos e

ininterruptos, a partir de sua assinatura, podendo o mesmo ser prorrogado por igual período ou rescindido, conforme interesse público, de acordo com a Lei Federal nº 8.666/93 e suas posteriores alterações

§2.º Os valores propostos serão reajustados, após um ano de vigência, pelo índice acumulado da variação do ICTI (Índice de Custo de Tecnologia da Informação) ou outro índice oficial que vier a substituí-lo.

§3.º O acesso ao serviço deverá ser disponibilizado em até 05 (cinco) dias corridos após o **recebimento da nota de empenho.**

§4.º Produtos entregues por meio de download ou aceso direto a um endereço da internet, a contratada deverá enviar um e-mail para o sti.pmsm@gmail.com , com todas as informações necessárias para realizar a utilização do produto/serviço objeto desta contratação.

§5.º No prazo máximo de 2 (dois) dias, contados da assinatura do contrato, a contratada deverá realizar reunião inicial de gestão do contrato.

§6.º Deverão estar presentes na reunião o preposto e um integrante da equipe técnica da contratada.

§7.º A pauta da reunião deverá abordar o planejamento detalhado da implantação da solução contratada, além das condições contratuais.

§8.º Os serviços deverão ser prestados em conformidade com as especificações deste Edital e seus anexos. Sendo constatada qualquer irregularidade, o prestador deverá concluir os serviços dentro das condições ideais, cujo prazo será determinado no ato pelo responsável do recebimento e imediatamente comunicado à Secretaria de Município para que seja(m) adotada(s) a(s) sanção(ões) cabível.

§9.º A Contratada será responsável por realizar uma consultoria e revalidação das regras do Firewall Fortinet FG-1100E, sendo emitido um relatório com as alterações realizadas na configuração. Esta consultoria e revalidação deverá ser feita com base nas orientações fornecidas pela Fortinet na consultoria Incident Readiness.

§10.º A Contratada deverá configurar as seguintes soluções Fortinet.

- FortiAuthenticator com licença SSO;
- FortiTokenMobile;
- FortiAnalyzer;
- FortiClient EMS com função de ZTNA;
- FortiEDR.

§11.º A Contratada será responsável por configurar por completo cada uma das soluções acima especificadas, sendo dado como aceito o funcionamento quando um total de 10% (dez) do total de licenças esteja plenamente em funcionamento. A Contratada deverá fazer um repasse de conhecimento para a equipe técnica da Contratante de modo que esta possa dar continuidade na implantação para os demais usuários/equipamentos.

§12.º A Contratada será responsável por configurar o FortiAuthenticator para validar os acessos dos usuários remotos que farão uso do FortiTokenMobile, ferramenta esta que ficará instalada em dispositivos móveis.

§13.º A Contratada será a responsável pela implantação do FortiAnalyzer e configuração / customização dos dispositivos fornecidos para o envio de logs para esta ferramenta de análise.

§14.º A Contratada será responsável por implantar o FortiClient EMS de modo que os usuários externos tenham uma segurança no acesso via esta ferramenta de confiança zero, a qual fará a validação de conformidade de dispositivos e usuários no acesso remoto.

§15.º A Contratada deverá criar templates, configurar servidores, máquinas e profiles do FortiEDR.

§16.º Deverá ser fornecido pela Contratada um treinamento de todas as soluções fornecidas, por um profissional com certificação mínima NSE7, com carga horária mínima de 24 (vinte e quatro) horas, para uma turma de até 6 (seis) pessoas.

§17.º O projeto deverá ser gerenciado por profissional Gerente de Projetos com certificação PMP do PMI ou com pós-graduação em Gerenciamento de Projetos.

§18.º O projeto deverá ser implantado por profissional com certificação mínima NSE7 do fabricante Fortinet.

§19.º A Contratada deverá considerar a participação presencial no projeto por no mínimo 5 (cinco) dias de um profissional com certificação Fortinet conjunto com o Gerente de Projetos para entendimento e consultoria inicial do ambiente envolvido neste projeto.

CLÁUSULA QUARTA– DA FISCALIZAÇÃO

O acompanhamento e a fiscalização do objeto desta Licitação serão exercidos por meio de um representante da Secretaria de Município de Finanças (Fiscal do Contrato) especificamente designado por portaria pela autoridade competente, de forma compartilhada com representantes indicados por cada Secretaria que compõe o presente processo licitatório, ao qual compete acompanhar, fiscalizar, conferir e avaliar a execução do objeto, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando o que for necessário à regularização das faltas, falhas, problemas ou defeitos observados, e os quais de tudo darão ciência à Contratada, conforme determina o art. 67, da Lei nº 8.666/1993, e suas alterações.

§1.º A fiscalização deverá ser de acordo com o regramento estipulado no Termo de Referência.

§2.º A fiscalização será exercida no interesse da Prefeitura Municipal de Santa Maria e não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica corresponsabilidade do Poder Público ou de seus agentes e prepostos.

§3.º Não obstante ser a Contratada a única e exclusiva responsável pela execução do objeto, a Contratante reserva-se o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização.

§4.º Cabe à Contratada atender prontamente e dentro do prazo estipulado quaisquer exigências da fiscalização inerentes ao objeto desta licitação, **sem que disso decorra qualquer ônus extra para a CONTRATANTE**, não implicando essa atividade de acompanhamento e fiscalização qualquer exclusão ou redução da responsabilidade da Contratada, que é total e irrestrita em relação ao objeto executado, inclusive perante terceiros, respondendo a mesma por qualquer falta, falha, problema, irregularidade ou desconformidade observada na execução do ajuste.

I - A atividade de fiscalização não resultará, tampouco, e **em nenhuma hipótese**, em corresponsabilidade da Contratante ou de seus agentes, prepostos e/ou assistentes.

§5.º O objeto do presente Edital deverá estar rigorosamente dentro das normas vigentes e das especificações estabelecidas pelo Município, sendo que a inobservância desta condição implicará a sua

recusa, bem como sua devida adequação e/ou substituição, sem que caiba à Contratada qualquer tipo de reclamação ou indenização.

§6.º As decisões e providências que ultrapassem a competência da fiscalização serão encaminhadas à autoridade competente da Contratante para adoção das medidas convenientes, consoante disposto no § 2º do art. 67, da Lei nº. 8.666/93.

CLÁUSULA QUINTA - DO RECURSO FINANCEIRO

As despesas decorrentes do presente Contrato correrão a conta do(s) seguinte(s) recurso(s) financeiro(s):

Secretaria de Município de Inovação e Tecnologia de Informação
Solicitação de Compra n.º 1662/2023
Projeto/Atividade: 2055
Subelemento Despesa: 3.3.90.40.99.00
Recurso: 2500

CLÁUSULA SEXTA - DO PAGAMENTO

§1.º O pagamento será efetuado em:

* 15 (quinze) dias consecutivos do recebimento da Nota Fiscal pelo fiscal do contrato. Para tanto a referida fatura deverá estar devidamente visada pelo responsável da Secretaria requisitante e entregue em até 05 dias para a Secretaria de Município de Finanças.

§2.º Deverá constar obrigatoriamente nas notas fiscais/faturas o número do empenho.

§3.º O pagamento será creditado em conta corrente da empresa, através de Ordem Bancária contra qualquer instituição bancária indicada na proposta, devendo para isto ficar explicitado o nome do ban-co, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

§4.º Os pagamentos serão concretizados em moeda vigente do país.

§5.º Para execução do pagamento de que trata este subitem, a Contratada deverá fazer constar como beneficiário/cliente da Nota Fiscal/Fatura correspondente, emitida sem rasuras, o Município de Santa Maria, CNPJ n.º 88.488.366/0001-00.

§6.º O pagamento somente será liberado após o recolhimento de eventuais multas que lhe tenham sido impostas em decorrência de inadimplência contratual.

§7.º Qualquer erro ou omissão havidos na documentação fiscal ou na fatura será objeto de correção pela empresa e haverá, em decorrência, suspensão do prazo de pagamento até que o problema seja definitivamente regularizado.

§8.º O Município reserva-se o direito de recusar o pagamento se, no ato do atesto, o objeto licitado não estiver de acordo com a especificação apresentada e aceita no Termo de Referência.

§9.º Na hipótese de atraso no pagamento da Nota Fiscal devidamente atestada, ao valor devido serão acrescentados juros calculados pro rata die, de acordo com a variação do Índice Nacional de Preços ao Consumidor Amplo - IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística - IBGE.

CLÁUSULA SÉTIMA - DOS DIREITOS E DAS OBRIGAÇÕES

Constituem direitos e obrigações das partes contratantes:

§1.º Dos Direitos

Constituem direitos: do CONTRATANTE, receber o objeto deste contrato nas condições avençadas e da CONTRATADA, perceber o valor ajustado na forma e no prazo convencionados.

§2.º Das Obrigações

I - Constituem obrigações do CONTRATANTE:

a) Exercer a fiscalização dos serviços;

b) Convocar a licitante para execução dos serviços;

c) Atestar as Notas Fiscais/Faturas correspondentes aos serviços prestados.

d) Proporcionar todas as condições necessárias para o cumprimento do objeto desta contratação.

e) Prestar informações e esclarecimentos que venham a ser solicitados pela Contratada, necessários ao cumprimento do objeto deste Termo de Referência.

f) Comunicar à Contratada qualquer irregularidade verificada no cumprimento do objeto, determinando, de imediato, a adoção de medidas necessárias à solução dos problemas.

g) Solicitar o reparo, a correção ou a substituição do objeto em que se verificarem vícios, defeitos ou incorreções.

h) Supervisionar a execução do objeto do Termo de Referência, exigindo presteza na execução e correção das falhas eventualmente detectadas;

i) Prestar à Contratada, em tempo hábil, as informações eventualmente necessárias à execução do objeto.

j) Impedir que terceiros executem o objeto deste Edital;

k) Efetuar o pagamento devido pela execução do objeto, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas.

I - Constituem obrigações do CONTRATADA:

a) Tomar todas as providências necessárias à fiel execução do objeto desta licitação;

b) Promover a execução do objeto dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis.

c) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto deste Contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução do serviço;

d) Manter durante a execução deste contrato todas as condições de habilitação e qualificação exigidas na licitação;

e) Responsabilizar-se pelas despesas decorrentes de frete, seguro e demais encargos;

f) Entregar o objeto a ser contratado, conforme convencionado, sem qualquer outro encargo ou despesa para o Contratante.

g) Se for o caso, a Contratada deverá fornecer informações contendo nome completo, CPF, cargo ou atividade exercida, lotação e local de exercício dos empregados na Contratante, para fins de divulgação na internet.

h) Prestar todos os esclarecimentos que lhe forem solicitados pela Contratante, atendendo prontamente a quaisquer reclamações;

i) Arcar com os ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de contravenção, seja por culpa sua ou de quaisquer de seus empregados ou prepostos, obrigando-se, outrossim, a quaisquer responsabilidades decorrentes de ações judiciais ou extrajudiciais de terceiros, que lhe venham a ser exigidas por força da lei, ligadas ao cumprimento do ajuste a ser firmado;

j) Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com a Contratante;

k) Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados quando da execução do objeto ou em conexão com ele, ainda que acontecido em dependência da Contratante, inclusive por danos causados a terceiros;

l) Obedecer às normas de segurança e higiene no trabalho e o fornecimento de todo o equipamento de proteção individual - EPI, necessário ao pessoal utilizado na prestação dos serviços. Fornecimento de vestimenta de trabalho e de todo o equipamento de proteção coletiva - EPC, necessário ao pessoal utilizado na prestação dos serviços;

m) Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionados à execução do objeto, originariamente ou vinculada por prevenção, conexão ou contingência;

n) Assumir a responsabilidade pelos encargos fiscais, comerciais e tributários resultantes da adjudicação deste processo licitatório;

o) Respeitar fielmente as Políticas, e Normas e Procedimentos de Segurança da Informação da Contratante.

p) Fornecer todos os materiais necessários à perfeita utilização dos equipamentos;

q) Não efetuar, sob nenhum pretexto, a transferência de qualquer responsabilidade para outras entidades, seja fabricantes, técnicos, subempreiteiros etc., sem a anuência expressa e por escrito da área administrativa da CONTRATANTE;

r) Responsabilizar-se pelo credenciamento e descredenciamento de acesso às dependências da CONTRATANTE, assumindo quaisquer prejuízos porventura causados por seus recursos técnicos;

s) Solicitar, por escrito, credenciamento e autorização de acesso para os recursos técnicos da Prefeitura Municipal de Santa Maria;

t) À CONTRATADA é vedado prestar informações a terceiros sobre a natureza ou andamento do fornecimento, objeto do Contrato, ou divulgá-los através da imprensa escrita, falada, televisada e/ou outro meio qualquer de divulgação pública, salvo autorização expressa da CONTRATANTE;

u) A Contratada deverá cumprir integralmente a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), no que couber.

Aceitar, nas mesmas condições do ajuste, os acréscimos ou supressões que se fizerem no objeto, de até 25% (vinte e cinco por cento) de seu valor

CLÁUSULA OITAVA - DA INEXECUÇÃO DO CONTRATO

A CONTRATADA reconhece os direitos do CONTRATANTE, em caso de rescisão administrativa, previstos no Art. 77 e seguintes, da Lei n.º 8.666/93.

CLÁUSULA NONA - DA RESCISÃO

Este contrato poderá ser rescindido:

a) Unilateralmente do CONTRATANTE, nos casos dos incisos I a XII e XVII do Art. 78, da Lei Federal n.º 8.666/93;

b) Amigavelmente, por acordo entre as partes, reduzindo a termo no processo de licitação, desde que haja conveniência para o CONTRATANTE;

c) Judicialmente, nos termos da legislação.

PARAGRAFO ÚNICO – A rescisão deste contrato implicará em retenção de créditos decorrentes da contratação, até o limite dos prejuízos causados ao CONTRATANTE, na forma que o mesmo determinar.

CLÁUSULA DÉCIMA - DO REAJUSTAMENTO DOS PREÇOS

Os preços sofrerão reajustes, desde que ultrapassados 12(doze) meses, conforme determina o §1.º do art. 2.º da Lei Federal n.º 10.192, de 14 de fevereiro de 2001.

PARAGRAFO ÚNICO – Os valores propostos serão reajustados, após um ano de vigência, pelo índice acumulado da variação do ICTI (Índice de Custo de Tecnologia da Informação) ou outro índice oficial que vier a substituí-lo.

CLÁUSULA DÉCIMA PRIMEIRA - DAS PENALIDADES E DAS MULTAS

Se a CONTRATADA recusar-se a prestar os serviços injustificadamente, serão convocados os demais licitantes, na ordem de classificação, para fazê-lo, sujeitando-se o licitante desistente às penalidades, sem prejuízo da aplicação de outras cabíveis.

PARÁGRAFO ÚNICO – Na hipótese de descumprimento parcial ou total da CONTRATADA das obrigações contratuais assumidas, ou a infringência de preceitos legais pertinentes, o CONTRATANTE poderá, garantida a prévia e ampla defesa, aplicar, segundo a gravidade da falta cometida, as seguintes sanções:

I - Advertência formal, por intermédio do setor competente, quando ocorrer o descumprimento das exigências editalícias que não justifiquem a aplicação de penalidade mais grave.

II - Multa equivalente a 0,5% (zero vírgula cinco por cento) sobre o valor total do contrato por dia de atraso injustificado ou por inobservância de qualquer obrigação assumida no presente instrumento:

a) O atraso na prestação dos serviços sujeitará a CONTRATADA ao pagamento de multa no percentual acima, por dia de atraso, até o limite máximo de 10% sobre o valor total do contrato, sem prejuízo das demais sanções previstas neste instrumento;

b) A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório, e a sua cobrança não isentará a CONTRATADA da obrigação de indenizar eventuais perdas e danos;

c) A multa aplicada a CONTRATADA e os prejuízos causados à Prefeitura Municipal de Santa Maria serão deduzidos de qualquer crédito a que tenha direito a CONTRATADA, cobrados diretamente ou judicialmente.

III - Multa de até 5% (cinco por cento) sobre o valor total do contrato no caso de inexecução parcial e 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto contratado.

IV - Suspensão do direito de licitar e contratar com a Administração, por período a ser definido na oportunidade, de acordo com a natureza e a gravidade da falta, respeitado o limite legal de 24 (vinte e quatro) meses, sem prejuízo da aplicação de multa, podendo ser aplicada quando:

a) apresentação de documentos falsos ou falsificados;

b) recusa injustificada em retirar o pedido de compra ou documento equivalente, dentro do prazo estabelecido pela Prefeitura Municipal de Santa Maria;

c) reincidência de descumprimento das obrigações assumidas no contrato acarretando prejuízos para a Prefeitura de Santa Maria, especialmente aquelas relativas às características dos bens/serviços, qualidade, quantidade, prazo ou recusa de prestação dos serviços, ressalvados os casos fortuitos ou de força maior, devidamente justificados e comprovados;

d) reincidência na aplicação das penalidades de advertência ou multa;

e) irregularidades que acarretem prejuízo à Prefeitura de Santa Maria, ensejando frustração deste contrato ou impedindo a realização de ato administrativo por parte do Município de Santa Maria;

f) prática de atos ilícitos, demonstrando não possuir idoneidade para licitar e contratar com a Prefeitura Municipal de Santa Maria;

g) condenação definitiva por praticar fraude fiscal no recolhimento de quaisquer tributos.

V - Declaração de inidoneidade para licitar e contratar com a Administração Pública, em função da natureza ou gravidade da falta cometida, sem prejuízo de multas incidentes.

CLÁUSULA DÉCIMA SEGUNDA - DO AMPARO LEGAL E LEGISLAÇÃO APLICÁVEL

A lavratura do presente contrato decorre da realização de Pregão, realizado com fundamento na Lei Federal n.º 10.520/2002, Decreto Municipal n.° 072/2015, e, subsidiariamente, na Lei Federal n.º 8.666/93.

PARÁGRAFO ÚNICO – A execução deste contrato, bem como os casos nele omissos, regular-se-ão pelas cláusulas contratuais e pelos preceitos de direito público, aplicando-lhes, supletivamente, os princípios de teoria geral dos contratos e as disposições de direito privado, na forma do art. 54, da Lei nº 8.666/93, combinado com o inciso XII, do art. 55, do mesmo diploma legal.

CLÁUSULA DÉCIMA TERCEIRA - DA VINCULAÇÃO AO EDITAL

Este Contrato fica vinculado aos termos da proposta da CONTRATADA e edital de licitação.

CLÁUSULA DÉCIMA QUARTA - DO FORO

Fica eleito o Foro da Comarca de Santa Maria - RS para dirimir dúvidas ou questões oriundas do presente contrato.

CLÁUSULA DÉCIMA QUINTA - DAS DISPOSIÇÕES FINAIS

E, por estarem justos e contratados, firmam o presente em 02 (duas) vias de igual teor e forma.

Gabinete do Prefeito Municipal de Santa Maria, Estado do Rio Grande do Sul, aos ___ (_____) dias do mês de _____ do ano de 2023.

_____
Jorge Cladistone Pozzobom
Prefeito Municipal
Contratante

_____
Representante Legal
Contratada.