Fundação Educacional do Município de Assis
Campus "José Santilli Sobrinho"

EDITAL Nº 010/2020
PROCESSO LICITATÓRIO Nº 012/2020
CONVITE Nº 004/2020

TIPO DE LICITAÇÃO: MENOR PREÇO
REGIME DE EXECUÇÃO: EMPREITADA POR PREÇO GLOBAL

ABERTURA	ENCERRAMENTO	HORÁRIO
14/02/2020	27/02/2020	09H30MIN

LOCAL: Sede da Fundação Educacional do município de Assis, Sala da Seção de Materiais – Bloco III / Avenida Getúlio Vargas, 1200, Vila Nova Santana, município de Assis, Estado de São Paulo.
OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

I - PREÂMBULO

A Comissão de Licitações da FEMA - Fundação Educacional do Município de Assis, Estado de São Paulo, designada pela Portaria nº 01 de 06/01/2020, no uso de suas atribuições legais, comunica a abertura do processo licitatório na modalidade CONVITE, tipo MENOR PREÇO, com a finalidade de CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, conforme especificado no Anexo I, que integra o presente edital.

II - FUNDAMENTO LEGAL

Esta licitação será regida pela Lei Federal nº 8.666/93, atualizada pela Lei Federal nº 8.883/94, e suas alterações com a devida observância das disposições legais estabelecidas nos artigos 42 a 45 da Lei Complementar nº 123/2006 e Decreto nº 6.204/07 e nos termos e condições fixadas nesse EDITAL e seus anexos.

III - DAS CONDIÇÕES DE PARTICIPAÇÃO

3.1. Poderão participar do certame todos os interessados do ramo de atividade pertinente ao objeto da contratação que atenderem a todas as exigências, inclusive quanto à documentação, constantes deste Edital e seus Anexos.

3.2. Empresa NÃO CONVIDADO, que manifestar interesse em participar do certame, com antecedência mínima de 24 (vinte e quatro) horas da data de abertura, conforme dispõe o art. 22, § 3º da Lei 8.666/93, deverá apresentar toda a documentação no dia do certame, na forma indicada no

presente edital.

3.2.1. Considerar-se-á como manifestação de interesse a solicitação por escrito, protocolado junto a esta Comissão Permanente de Licitações da FEMA. (modelo Anexo VIII)

3.3. A participação na licitação implica na aceitação integral e irretratável dos termos deste Edital, bem como na observância dos regulamentos, normas e disposições legais pertinentes.

IV - DA FORMA DE PREENCHIMENTO EXTERNO DOS ENVELOPES

4.1. Em sua parte externa, os envelopes deverão conter as seguintes informações:

EDITAL N.º 010/2020 CONVITE N.º 004/2020 ABERTURA DIA 27/02/2020 às 09h30min. **ENVELOPE 01 – DOCUMENTOS DE HABILITAÇÃO** RAZÃO SOCIAL DA PROPONENTE CNPJ: ENDEREÇO: FONE/FAX: E-MAIL:

EDITAL N.º 010/2020 CONVITE N.º 004/2020 ABERTURA DIA 27/02/2020 às 09h30min. **ENVELOPE 02 – PROPOSTA DE PREÇOS** RAZÃO SOCIAL DA PROPONENTE CNPJ: ENDEREÇO: FONE/FAX: E-MAIL:

V - APRESENTAÇÃO E CONTEÚDO DOS DOCUMENTOS DE HABILITAÇÃO

5.1. No **ENVELOPE Nº 01 – DOCUMENTOS** – deverão ser apresentados os documentos para habilitação, em original ou por cópia autenticada por tabelião de notas ou pelos membros da Comissão de Licitações, conforme o art. 32 da Lei Federal nº 8.666/93, em envelope lacrado e opaco, devendo conter:

5.1.1. Relativos à Habilitação Jurídica, conforme o caso:

5.1.1.1. Registro comercial, para empresa individual; ou

5.1.1.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de

sociedades por ações, acompanhado de documentos de eleição de seus administradores; ressaltando que os documentos deverão estar acompanhados de todas as alterações ou da consolidação respectiva, conforme legislação em vigor.

5.1.1.3. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício.

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

5.1.1.5. Caso o licitante vencedor do certame seja microempresa (ME) ou empresa de pequeno porte (EPP) e tenha qualquer restrição relativa à documentação apresentada para sua regularidade fiscal exigidas no subitem 5.1.2. terá o prazo de 05 (cinco) dias úteis contados a partir da sua declaração de vencedor da licitação, para sanar a irregularidade pendente, sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções cabíveis.

5.1.1.6. As microempresas (ME) e empresas de pequeno porte (EPP) deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

5.1.1.7. Os documentos apresentados por empresas que possuam filiais deverão possuir a titularidade do licitante (mesma razão social e mesmo CNPJ), exceto os documentos de qualificação técnica, que poderão trazer CNPJ da filial ou da matriz, conforme o caso.

5.1.2. Relativos à Regularidade Fiscal e Trabalhista:

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

5.1.2.2 Certidão Conjunta Negativa ou Certidão Conjunta Positiva com Efeitos de Negativa, relativos a Tributos Federais e à Dívida Ativa da União;

5.1.2.3. Prova de regularidade, em plena validade, para com a Fazenda Estadual, do domicílio ou sede do licitante, ou outra equivalente na forma da lei;

5.1.2.4. Certidão Negativa ou Positiva com Efeitos de Negativa de Tributos Mobiliários, expedida pela Secretaria Municipal de Finanças;

5.1.2.5 Prova de regularidade para com o Fundo de Garantia por Tempo de Serviço - FGTS (Certificado de Regularidade Fiscal - CRF), em plena validade;

5.1.2.6 Prova de regularidade para com o Tribunal Superior do Trabalho (Certidão Negativa de Débitos Trabalhistas - CNDT), em plena validade;

5.1.3. Relativos à Qualificação Econômico-Financeira:

5.1.3.1. Certidão negativa de falência, ou recuperação judicial, ou liquidação judicial, ou de execução patrimonial, conforme o caso, expedida

pelo distribuidor da sede do licitante, ou do seu domicílio, dentro do prazo de validade previsto na própria certidão. Caso as certidões sejam apresentadas sem indicação do prazo de validade, serão consideradas válidas, para este certame, aquelas emitidas há no máximo 60 (sessenta) dias da data estipulada para a abertura da sessão.

5.1.4. Declarações:

5.1.4.1. Declaração de inexistência de fato que impeça a empresa de participar da licitação, bem como de que não foi declarada inidônea ou suspensa de contratar com o poder público (ANEXO III);

5.1.4.2. Declaração de que não possui em seu quadro de pessoal menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, ou menor de 14 (catorze) anos em qualquer trabalho, salvo na condição de aprendiz (Lei 9.854/99), (ANEXO IV);

5.1.4.3. Para obter os benefícios do Artigo 43 da Lei Complementar n. 123/06, na qualidade de microempresa (ME) ou empresa de pequeno porte (EPP), deverá apresentar declaração (ANEXO V) e toda documentação comprobatória.

5.2. Os documentos necessários à habilitação poderão ser apresentados em original, por qualquer processo de cópia autenticada por cartório competente ou por servidor da Administração ou publicação em órgão da imprensa oficial, ou através de impresso informatizado obtido via Internet.

5.3. Na hipótese de não constar prazo de validade nos documentos apresentados, a Administração aceitará como válidos os expedidos até 90 (noventa) dias imediatamente anteriores à data de apresentação das propostas, se outro prazo de validade não constar nos documentos.

5.4. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se 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.

VI - APRESENTAÇÃO E CONTEÚDO DA PROPOSTA

6.1. No **ENVELOPE Nº 02, a PROPOSTA** deverá ser apresentada datilografada ou digitada sem emendas nem rasuras e atender a todas as exigências contidas neste Edital; ao final, deve ser identificada, assinada e acondicionada em envelope opaco e lacrado.

6.2. O valor ofertado deverá ser fixo e irreajustável, expresso em moeda corrente nacional, já incluídos impostos, taxas, e quaisquer outras despesas, diretas ou indiretas, sem inclusão de qualquer encargo financeiro ou previsão inflacionaria, devendo constar:

6.2.1. Identificação do proponente (endereço, endereço eletrônico, telefone, e-mail, CNPJ/CPF) e referência a esta licitação;

6.2.2. Descrição dos serviços e dos produtos, de acordo com o Anexo I deste EDITAL;

6.2.3. Valor unitário, total da proposta;

6.2.4. Validade da proposta de, no mínimo, 60 (sessenta) dias contados a partir da data de sua apresentação.

6.2.5. As licitantes deverão apresentar suas propostas usando, preferencialmente, o modelo sugerido no anexo II.

6.3. Não serão aceitas propostas com opções.

6.4. A proposta, depois de aberta, se acha vinculada à licitação pelo seu prazo de validade, não sendo admitidas quaisquer inclusões ou alterações no sentido de sanar falhas ou omissões, assim como não será permitida a sua retirada ou desistência por parte do proponente.

6.5. Ao apresentar a proposta, o proponente, automaticamente aceita e se sujeita a todas as cláusulas e condições do presente edital.

VII - DA ABERTURA DOS ENVELOPES

7.1. Os envelopes deverão ser entregues **até às 09h30min do dia 27/02/2020** no Setor de Materiais - Bloco III da FEMA, na Avenida Getúlio Vargas, 1200.

7.2. A Comissão iniciará os trabalhos em sessão pública no dia, hora e local indicados no preâmbulo deste Edital e no item supracitado.

7.3. Os envelopes contendo os documentos de habilitação serão abertos pela Comissão, que, após conferi-los, darão vista aos licitantes que desejarem.

7.4. Serão considerados habilitados os licitantes que atenderem ao estabelecido nas cláusulas VI e VII deste Edital.

7.5. A inabilitação do licitante implica perda do seu direito de participar das fases subsequentes.

7.6. Se todas as empresas forem desclassificadas (fase de habilitação) ou se as forem propostas, a Comissão poderá fixar o prazo de 03 (três) dias úteis para que os licitantes apresentem nova documentação ou nova proposta, escoimada das causas que tenham originado a desclassificação.

VIII - DOS RECURSOS ORÇAMENTÁRIOS

8.1. A dotação orçamentária correrá por conta de verbas codificadas sob os números:

3.3.90.40.00.00.00 – Serviços de tecnologia da informação e comunicação
3.3.90.40.99.00.00 – Outros serviços de tecnol. da Inf. eCom. – Pessoa Jurídica
Códigos Reduzidos 116 e 513

8.2. O valor orçado para a contratação é de R$ 156.000,00 (cento e cinquenta e seis mil).

IX - DO JULGAMENTO

9.1. O julgamento e a classificação das propostas serão efetuados pela

C.L. FEMA
FLS. nº 136

Comissão de Licitações da FEMA, pelo critério de MENOR PREÇO.

9.2. A Comissão de Licitação verificará o porte das empresas licitantes classificadas. Havendo microempresas ou empresas de pequeno porte participantes, proceder-se-á a comparação com os valores da primeira colocada, se esta for empresa de maior porte, 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.

9.3. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 10% (dez por cento) acima da proposta de menor preço serão consideradas empatadas com a primeira colocada.

9.4. 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 05 (cinco) minutos, caso esteja presente na sessão ou no prazo de 02 (dois) dias, contados da comunicação da comissão de Licitação, na hipótese de ausência. Neste caso, a oferta deverá ser escrita e assinada para posterior inclusão nos autos do processo licitatório.

9.5. Caso a microempresa ou empresa de pequeno porte classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresas e empresas de pequeno porte que se encontrem naquele intervalo de 10% (dez por cento), na ordem de classificação, para o exercício do mesmo direito, nos mesmos prazos estabelecidos no subitem anterior.

9.6. Caso sejam identificadas propostas de preços idênticos de microempresa ou empresa de pequeno porte empatadas na faixa de até 10% (dez por cento) sobre o valor cotado pela primeira colocada, a Comissão de Licitação convocará os licitantes para que compareçam ao sorteio na data e horário estipulados, para que se identifique aquela que primeiro poderá reduzir a oferta.

9.7. Havendo êxito no procedimento de desempate, será elaborada a nova classificação das propostas para fins de aceitação do valor ofertado. Não sendo aplicável o procedimento, ou não havendo êxito na aplicação deste, prevalecerá a classificação inicial.

9.8. Na hipótese de ser verificada absoluta igualdade entre as propostas de menor valor, o desempate será decidido por sorteio, após convocação das licitantes.

9.9. Ainda nesta fase serão desclassificadas as propostas que não satisfaçam integralmente ao estabelecido pelo presente Edital, as que apresentarem preços excessivos ou manifestamente inexequíveis.

C.L. FEMA
FLS. nº 137

9.10. Após as desclassificações/classificações, todas as propostas classificadas serão organizadas em ordem crescente de preços, com a finalidade de eleger a proposta de menor valor como sendo a mais bem classificada.

9.11. O resultado do julgamento será divulgado nos termos legais, abrindo-se vistas dos autos e prazo de recursos nos termos da Lei n.º 8.666/93.

X - DA CONTRATAÇÃO

10.1. A contratação decorrente desta licitação será formalizada mediante celebração de termo de Contrato, cuja minuta integra este Convite como Anexo IX;

10.2. O prazo de vigência contratual será de 12 (doze) meses contados da data da assinatura do contrato, podendo ser prorrogado na forma da Lei;

12.2.1. Caso o contrato venha a ser prorrogado, o preço contratado poderá ser reajustado pelo Índice Geral de Preços do Mercado (IGP-M) acumulado em 12 (doze meses).

10.3. O licitante adjudicatário será convocado oficialmente para assinatura do contrato e/ou retirar nota de empenho, devendo comparecer no prazo de 5 (cinco) dias úteis contados da data da convocação, podendo ser prorrogado, por uma vez, por igual período, quando solicitado pela parte durante o seu transcurso e desde que ocorra motivo justificado aceito pela Administração.

10.4. Decorridos os prazos acima citados e, não tendo o licitante vencedor comparecido ao chamamento, perderá o direito à contratação, estando sujeita às penalidades previstas no item 13 deste edital.

10.5. Verificada a hipótese expressa no subitem 10.4, bem como em caso de perda dos requisitos de habilitação constante neste edital, serão convocados os licitantes remanescentes, observada a ordem de classificação e requisitos de habilitação, até a efetiva contratação.

XI - DO LOCAL E DAS CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

11.1. O objeto desta licitação deverá ser executado na sede da FEMA localizada no Município de Assis, Estado de São Paulo à Avenida Getúlio Vargas, n.º 1.200, Vila Nova Santana, e, nas condições estabelecidas no Termo de Referência (Anexo I) deste edital, correndo por conta da CONTRATADA as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto do contrato.

11.1.1. O horário conveniente para a realização dos serviços deverá ser agendado com o funcionário designado pela Fundação Educacional do Município de Assis – FEMA, adequando-se às prioridades da Instituição.

11.1.2. O acompanhamento e a fiscalização do serviço serão efetuados de

acordo com o artigo 67 da Lei 8.666/93 e alterações incluídas pela Lei 9.648/98, por um representante da FEMA ou do respectivo local dos serviços, designado pela Direção Executiva.

11.2. O prazo para ativação dos serviços do presente certame é de até 30 (trinta) dias corridos.

11.3. A CONTRATADA deverá enviar seus técnicos devidamente identificados, com crachá e /ou uniformizados, provendo-os dos Equipamentos de Proteção Individual - EPIs, responsabilizando-se pelo uso e retirando do local de execução dos serviços aqueles que se recusarem a fazer uso dos equipamentos.

11.4. O objeto da licitação será recebido provisoriamente mediante recibo ou termo circunstanciado.

11.5. O recebimento definitivo não exime a contratada de sua responsabilidade, na forma da Lei, pela qualidade, correção e segurança dos bens adquiridos.

11.6. A contratante rejeitará, no todo ou em parte, serviço ou fornecimento executado em desacordo com o Termo de Referência (ANEXO I), cabendo à licitante vencedora as penalidades previstas no item 14 deste Edital, bem como o disposto na Lei federal n.º 8.078 de 11/09/90 "Código de Defesa do Consumidor".

XII - DO PAGAMENTO

12.1. O pagamento será efetuado à CONTRATADA, no prazo máximo de 05 (cinco) dias úteis, contados do primeiro dia seguinte ao recebimento da documentação fiscal completa (Nota Fiscal, Fatura e demais documentos exigíveis).

12.2. A constatação de irregularidades na execução deste ajuste motivará o desconto da importância correspondente ao descumprimento, sem prejuízo da eventual rescisão e aplicação das penalidades fixadas no item 14 deste edital.

12.3. A FEMA efetuará pagamento através do sistema bancário.

12.4. Não será admitida proposta com condição de pagamento antecipado ou de prazo contado da data de emissão da nota fiscal.

12.5. Nenhum pagamento será efetuado ao licitante vencedor enquanto pendente de liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

XIII - DAS SANÇÕES

13.1. A recusa injustificada da CONTRATADA em aceitar ou retirar o termo de contrato ou documento equivalente, dentro do prazo estabelecido caracteriza o descumprimento total da obrigação assumida, sujeita-o, sem prejuízo das sanções previstas na Lei Federal nº 8.666/93, as sanções de:

I - advertência;
II - multa;
III - suspensão temporária do direito de participar em licitação e impedimento de contratar com a FEMA, pelo prazo de 02 (dois) anos;
IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação.

13.1.1. A multa prevista no inciso II do item 13.1. será aplicada nos seguintes percentuais:

a) Na hipótese de inexecução total das obrigações, multa de 20% (vinte por cento) do valor total atualizado do ajuste;

b) Na hipótese de inexecução parcial das obrigações, multa de 10% (dez porcento) sobre o valor da obrigação não cumprida.

13.2. Se o licitante deixar de entregar a documentação ou apresentá-la falsamente, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará, pelo prazo de até 5 (cinco) anos, impedido de contratar com a Administração Pública, sem prejuízo das multas previstas no edital e das demais cominações legais.

13.3. As multas e outras sanções aplicadas só poderão ser relevadas se ocorrer caso fortuito ou motivo de força maior, devidamente justificado e comprovado, a critério do Diretor Executivo da FEMA.

13.4. Pelo atraso injustificado, sem prejuízo do disposto no §1° do artigo 86 da Fei Federal n. 8.666/93, sujeitará a CONTRATADA à multa diária de mora equivale a 0,1% (um décimo por cento) sobre o valor não cumprido.

13.5. O valor da multa será automaticamente descontado de pagamento presente, anterior ou futuro a que o adjudicatário tenha direito.

13.6. Os atrasos injustificados superiores a 30 (trinta) dias corridos serão obrigatoriamente considerados inexecução total ou parcial, estando a CONTRATADA sujeita as sanções previstas nos item 13.1.1.

13.7. Não havendo possibilidade dessa forma de compensação, o valor da multa, atualizado pela variação do Índice Geral de Preços de Mercado - IGPM, deverá ser pago pelo inadimplente na tesouraria da FEMA. Na ocorrência do não pagamento, o valor será cobrado judicialmente.

13.8. A aplicação das sanções acima identificadas será realizada de forma cumulativa.

13.9. Independentemente das sanções retro, a CONTRATADA ficará sujeita, ainda, à composição das perdas e danos causados à Administração e decorrentes de sua inadimplência, bem como arcará com a correspondente diferença de preços verificada em nova contratação, na

hipótese de os demais classificados não aceitarem a contratação pelos mesmos preços e prazos fixados pelo inadimplente.

13.10. São assegurados, nos termos legais, os prazos para exercício do direito da ampla defesa e do contraditório, na aplicação das sanções.

XIV – DA RESCISÃO

14.1. O contrato poderá ser rescindido de pleno direito, quando:

14.1.1. A inexecução total ou parcial do CONTRATO enseja a sua rescisão pela CONTRATANTE, com as consequências previstas nos artigos 77 e 80 da Lei Federal nº 8.666/93, sem prejuízo da aplicação das penalidades a que alude o artigo 87 da mesma Lei;

14.1.2. Constituem motivos para rescisão os previstos no artigo 78 da Lei Federal nº 8666/93 e alterações posteriores.

14.1.3. Nos termos do art. 79 da Lei Federal nº 8.666/93, a rescisão contratual poderá ser:

a) Determinada por ato unilateral e escrito da CONTRATANTE, nos casos enumerados nos incisos I, XII e XVII do artigo 78 da Lei nº 8.663/93;

b) Amigável, por acordo entre as partes, mediante autorização escrita e fundamentada da CONTRATADA, reduzida a termo, desde que haja conveniência da CONTRATANTE;

c) Judicial, nos termos da legislação;

14.1.4. Quando a rescisão ocorrer com base nos incisos XII a XVII do artigo 78 da Lei Federal nº 8.666/93, sem que haja culpa da CONTRATADA, será esta ressarcida dos prejuízos regularmente comprovados que houver sofrido, tendo ainda direito aos pagamentos devidos pela execução do CONTRATO até a data da rescisão.

XV. DA GARANTIA DOS SERVIÇOS

15.1. A licitante/adjudicatária deverá oferecer GARANTIA de no mínimo 1 (um) ano para os serviços de instalação, a contar da data de recebimento definitivo dos serviços.

15.1.1. Durante o prazo de garantia dos serviços, a CONTRATADA obriga-se a adotar medidas corretivas necessárias, sem ônus para a CONTRATANTE, designando profissional habilitado e experiente, no prazo de 10 (dez) dias úteis, contados a partir do primeiro dia útil subsequente aquele do recebimento da notificação expedida pela FEMA.

15.2. A CONTRATADA deverá, obrigatoriamente, entregar termo de garantia no ato de conclusão dos serviços, sob pena de não lhe ser fornecido sequer o recebimento provisório.

15.3. A CONTRATADA durante o prazo da garantia da execução dos serviços é responsável pela solidez e segurança dos serviços executados, bem como eventuais vícios ocultos.

XVI - DOS PEDIDOS DE ESCLARECIMENTOS E IMPUGNAÇÃO DO EDITAL

16.1. Os pedidos de esclarecimentos, relacionados com a Licitação, poderão ser realizados por qualquer pessoa, inclusive licitante, e deverão ser enviados à Comissão Permanente de Licitação, até 02 (dois) dias úteis antes da data fixada para a abertura dos envelopes.

16.2. Os pedidos de esclarecimentos deverão ser solicitados por escrito, e encaminhados a FEMA, aos cuidados da Comissão Permanente de Licitação, na Avenida Getúlio Vargas, n.º 1.200, Vila Nova Santana, Assis/SP – CEP 19807-130, ou pelo e-mail: licitacaofema@gmail.com.

16.3. Nos pedidos de esclarecimentos, os interessados deverão se identificar mencionando (o seu nome ou o nome do representante legal, com nº do CPF e do documento de identidade - respectivos); e disponibilizar as informações para contato (endereço completo, telefone, fax e e-mail).

16.4. Os esclarecimentos serão prestados pela Comissão Permanente de Licitação, por escrito, por meio de e-mail àqueles que enviaram recibo de retirada do Convite.

16.5. É facultado a qualquer cidadão impugnar, por escrito, os termos do presente Edital de Convite por irregularidade na aplicação da Lei n.º 8.666/93 e suas alterações, em até 2 (dois) dias úteis antes da data fixada para recebimento e abertura dos envelopes Documentação e Proposta.

16.6. Decairá do direito de impugnar os termos deste Edital o (a) licitante que não o fizer até o 2º (segundo) dia útil que anteceder à data marcada para abertura dos envelopes, apontando as falhas ou irregularidades que o viciarem, hipótese em que tal comunicação não terá efeito de recurso.

16.7. O (a) interessado (a) deverá apresentar instrumento de impugnação dirigido à Comissão Permanente de Licitação, a ser protocolizado junto à FEMA no horário de 08h às 12h e das 14h às 17h, fundamentando o alegado, e, se for o caso, juntar as provas que se fizerem necessárias.

16.8. Acolhida a petição contra o ato convocatório, a decisão será comunicada aos interessados.

16.9. Os pedidos de impugnações e esclarecimentos, bem como as respectivas respostas, serão divulgados pela Comissão Permanente de Licitação no site: www.fema.edu.br.

16.10. As respostas aos pedidos de impugnações e esclarecimentos aderem a esse Edital tal como se dele fizessem parte, vinculando a Administração e os (as) licitantes.

16.11. As interpretações, correções e/ou alterações deste instrumento convocatório, elaboradas pela FEMA, serão comunicadas pela mesma forma que se deu o texto original do Convite, observadas as condições do §4º do art. 21 da Lei Federal nº 8.666/93.

XVII - DO DIREITO DE RECURSO

17.1. Dos atos praticados pela Comissão de Licitações no processamento da licitação, cabem recursos hierárquicos nas formas e prazos estabelecidos pelo artigo 109 da Lei Federal nº 8.666/93, que deverá ser protocolado junto ao Setor de Materiais - Licitações, à Avenida Getúlio Vargas, 1200, devendo o mesmo estar claramente endereçado à referida Comissão.

XVIII - DISPOSIÇÕES GERAIS

18.1. Antes do recebimento dos envelopes, este edital poderá ser alterado por razões de interesse público ou por exigência legal. Em qualquer caso, se a modificação afetar a apresentação dos documentos de habilitação e a formulação das propostas, a FEMA informará aos interessados que tenham retirado o Edital as modificações no texto original, fixando nova data para apresentação, exceto quando, inquestionavelmente, as alterações não afetarem a habilitação ou a formulação das propostas.

18.2. Não serão aceitas propostas enviadas via FAC-SÍMILE.

18.3. À FEMA fica reservado o direito de rejeitar todas as propostas ou de, em qualquer fase do processo, anular ou revogar esta licitação, sem que, com isso, os participantes adquiram direito a indenizações ou compensações.

18.4. Após a entrega da proposta pelos licitantes não serão aceitos quaisquer adendos, acréscimos, supressões ou esclarecimentos sobre o conteúdo dos mesmos.

18.5. A critério da Comissão de Licitações poderão ser relevados erros ou omissões formais, desde que não resultem prejuízo para o entendimento das propostas.

18.6. É facultado à Comissão ou a autoridade superior, em qualquer fase da licitação, promover diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão de documentos ou informações que deverão constar originalmente da proposta.

18.7. Decairá do direito de impugnar os termos do edital perante a Administração o licitante que, tendo-o aceitado sem objeção, venha a apontar, depois da abertura dos envelopes, falhas ou irregularidade que o tenham viciado, hipótese em que a comunicação não terá efeito de recurso.

18.8. Das sessões públicas realizadas para esta licitação será lavrada ata circunstanciada dos trabalhos, onde serão registradas as impugnações fundamentadas porventura apresentadas pelos representantes legais presentes.

18.9. O Licitante fica obrigado a aceitar os acréscimos ou supressões que se fizerem na execução do objeto, de até 25% (vinte e cinco por cento), de acordo com o artº 65, § 1º da Lei Federal nº 8.666/93.

C.L. FEMA
FLS. nº 143

18.10. O EDITAL encontra-se disponível na Seção de Materiais da FEMA e na internet em www.fema.edu.br.

XIX – DOS ANEXOS

19.11. Integra o presente Edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Termo de Referência;
ANEXO II – Modelo Sugerido de Proposta Comercial;
ANEXO III – Modelo de Declaração de cumprimento das condições de habilitação
ANEXO IV - Modelo de Declaração de Inexistência de Fato Impeditivo para Licitar ou Contratar com a Administração
ANEXO V - Modelo de Declaração de Inexistência de Trabalho de Menor (Disposto do Inciso XXXIII Art.º 7º da Constituição Federal)
ANEXO VI - Modelo de Declaração para Microempresas e Empresa de Pequeno Porte
ANEXO VII – Declaração recebimento do edital
ANEXO VIII - Declaração de interesse em participação na licitação
ANEXO IX - Minuta de Contrato

Assis, 14 de fevereiro de 2020.

Eduardo Augusto Vella Gonçalves
Diretor Executivo

ANEXO I
TERMO DE REFERÊNCIA
PROCESSO LICITATÓRIO N.º 012/2020
CONVITE N.º 004/2020

1. OBJETO

1.1. A presente licitação tem como objeto a Contratação de empresa especializada na prestação de Serviços Gerenciados de Tecnologia da Informação como Serviços Gerenciados de Segurança da Informação devidamente descritos e caracterizados nas especificações técnicas presente abaixo:

1.1.1. Os equipamentos utilizados pela licitante vencedora para prestação dos serviços deverão ser novos, sem uso anterior, embalados, lacrados de fábrica e ainda em linha de produção em pleno funcionamento, e cobertos por garantia pelo respectivo fabricante durante toda a vigência do contrato.

1.1.2. Deverão ser apresentados juntamente com a proposta comercial catálogos, encartes, folhetos técnicos e manuais dos equipamentos, softwares e serviços ofertados, onde constem as especificações técnicas e a caracterização dos mesmos, permitindo a consistente avaliação dos itens.

1.1.3. O prazo para ativação dos serviços do presente certame é de até 30 (trinta) dias corridos.

1.1.4. O serviço deverá ser prestado durante o período de 12 (doze) meses podendo ser prorrogado por iguais períodos nos termos do inc. IV do art. 57 da 8.666/93.

LOTE - SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO		
ITEM	**DESCRIÇÃO**	**QTD**
1	Serviços Gerenciados de Segurança da Informação	1
2	Serviço de Proteção para Estações de Trabalho	1
3	Serviço de Suporte Técnico e Monitoramento de Infraestrutura	1
4	Serviço de Backup em Nuvem	1

1. <u>ITEM 1: Serviços Gerenciados de Segurança da Informação</u>

1.2 <u>Solução de Firewall de Próxima Geração</u>

1.2.1 A contratada deverá fornecer uma solução de firewall de próxima geração (NGFW – Next Generation Firewall) em alta disponibilidade, no modo Ativo-Passivo, ou seja, no mínimo um equipamento disponível para assumir o funcionamento automaticamente, caso o principal fique

indisponível;

1.2.2 Fornecer e substituir, em caso de necessidade, as peças defeituosas de todos os equipamentos fornecidos como serviço e efetuar os necessários ajustes sem ônus para o contratante desde que os danos causados não sejam de responsabilidade do contratante;

1.2.3 Os equipamentos devem ser iguais e suportar no mínimo as seguintes configurações e ser configuradas de acordo com ambiente:

1.2.4 Especificações Gerais:

1.2.4.1 O equipamento proposto deve fornecer logs e relatórios embarcados contendo no mínimo os itens abaixo:

1.2.4.1.1 Dashboard com informações do sistema:

1.2.4.1.1.1 Informações de CPU

1.2.4.1.1.2 Informações do uso da rede.

1.2.4.1.1.3 Informações de memória.

1.2.4.1.1.4 Informações de atividades de navegação.

1.2.4.1.1.5 Permitir visualizar número políticas ativas.

1.2.4.1.1.6 Visualizar número de usuários conectados remotamente.

1.2.4.1.1.7 Visualizar número de usuários conectados localmente.

1.2.4.2 Relatórios com informações sobre as conexões de origem e destino por países.

1.2.4.3 Relatórios informando as conexões dos hosts.

1.2.4.4 Visualizar relatórios por período de tempo, permitindo o agendamento e o envio destes relatórios por e-mail.

1.2.4.5 Permitir exportar relatórios para as seguintes extensões/plataformas:

1.2.4.5.1 PDF

1.2.4.5.2 HTML

1.2.4.6 Excel

1.2.4.7 Permitir visualizar relatório de políticas ativas associado ao ID da política criada.

1.2.4.8 Relatório que informe o uso IPSEC por host e usuário.

1.2.4.9 Relatório que informe o uso L2TP por host e usuário.

1.2.4.10 Relatório que informe o uso PPTP por usuários.

1.2.4.11 Relatório abordando eventos de VPN.

1.2.4.12 Proporcionar sistema de logs em tempo real, com no mínimo as seguintes informações:

1.2.4.12.1 Logs do sistema;

1.2.4.12.2 Logs das políticas de segurança;

1.2.4.12.3 Logs de autenticação;

1.2.4.12.4 Logs de administração do firewall NGFW.

1.2.4.12.5 Permitir ocultar dos relatórios usuários e IPs cadastrados.
1.2.4.13 Possuir no mínimo 8 interfaces 10/100/1000 base-T e 2 SFP 1GbE;
1.2.4.14 Possuir no mínimo 2 interfaces SFP+ 10GbE base-SR, com seus devidos transceivers e cabo de no mínimo 1 metro;
1.2.4.15 Deve suportar adição futura de no mínimo 2 interfaces 40GbE QSFP+;
1.2.4.16 Deve possuir no mínimo 2 portas que suportem by-pass;
1.2.4.17 A contratada deverá fornecer todos os cabos e seus acessórios necessários para atender os itens deste documento.
1.2.4.18 A solução proposta deve corresponder aos seguintes critérios de throughput máximo, considerando o tamanho do pacote UDP sendo 1518 byte:
1.2.4.18.1 Suportar no mínimo 6 (seis) Gbps de rendimento (throughput) de NGFW (next-generation firewall);
1.2.4.18.2 Suportar no mínimo 200.000 (duzentas mil) novas conexões por segundo;
1.2.4.18.3 Suportar no mínimo 17.500.000 (dezessete milhões e quinhentas mil) conexões simultâneas;
1.2.4.18.4 Possuir no mínimo 33 (trinta e três) Gbps de rendimento (throughput) do Firewall para pacotes UDP;
1.2.4.18.5 No mínimo 8.5 (oito inteiros e cinco décimos) Gbps de rendimento (throughput) do IPS;
1.2.4.18.6 Possuir no mínimo 3.2 (três inteiros e dois décimos) Gbps de throughput de VPN AES.
1.2.4.19 A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.
1.2.4.20 A solução proposta deve fornecer os relatórios diretamente no Firewall NGFW, baseados em usuário, não só baseado em endereço IP.
1.2.4.21 A solução proposta deve possuir no mínimo 180 GB de espaço em disco SSD para o armazenamento local de eventos e relatórios.
1.2.4.22 Possuir slot para adição de módulo de portas;
1.2.4.23 Possuir ao menos uma porta console RJ45 ou similar;
1.2.4.24 Número irrestrito de usuários/IP conectados.
1.2.4.25 O equipamento deve ter no máximo 2 (dois) U de altura para montagem em rack 19".

1.2.5 Especificações da Administração, Autenticação e Configurações em geral

1.2.5.1 A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e console.
1.2.5.2 A solução proposta deve ser capaz de importar e exportar

cópias de segurança (backup) das configurações, incluindo os objetos de usuário.

1.2.5.3 O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais e-mails pré-definidos, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano.

1.2.5.4 A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos.

1.2.5.5 A solução proposta deve suportar integrações com Active Directory, LDAP, Radius, eDirectory, TACACS+ e Banco de Dados Local para autenticação do usuário.

1.2.5.6 A solução proposta deve suportar em modo automático e transparente "Single Sign On" na autenticação dos usuários do active directory e eDirectory.

1.2.5.7 Suporte à autenticação do Chromebook.

1.2.5.8 Os tipos de autenticação devem ser, modo transparente, por autenticação NTLM e cliente de autenticação nas máquinas.

1.2.5.9 Fornecer clientes de autenticação para Windows, MacOS X, Linux 32/64.

1.2.5.10 Certificados de autenticação para iOS e Android.

1.2.5.11 A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual.

1.2.5.12 A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.

1.2.5.13 A solução proposta deve suportar NTP.

1.2.5.14 A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.

1.2.5.15 A solução proposta deve ter suporte multilíngue para console de administração web.

1.2.5.16 A solução proposta deverá suportar fazer um rollback de versão.

1.2.5.17 A solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.

1.2.5.18 A solução proposta deve suportar instalação de LAN by-pass no caso do firewall NGFW estar configurado no modo transparente.

1.2.5.19 A solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que o PPPoE mudar.

1.2.5.20 A solução proposta deve suportar SNMP v1, v2c.

1.2.5.21 A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.

1.2.5.22 A solução proposta deve ser baseada em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno "rollback" da cópia de segurança.

1.2.5.23 A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.

1.2.5.24 A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação).

1.2.5.25 A solução proposta deve ter suporte a ambientes de terminais (Microsoft) suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.

1.2.5.26 A solução proposta deve suportar:

1.2.5.26.1 Serviço de DHCP/DHCPv6;

1.2.5.26.2 Serviço de DHCP/DHCPv6 Relay Agent;

1.2.5.27 A solução proposta deve trabalhar como DNS/DNSv6 Proxy.

1.2.5.28 Gráficos, relatórios e ferramentas avançadas de apoio para troubleshooting.

1.2.5.29 Permitir exportar informações de troubleshooting para arquivo PCAP.

1.2.5.30 Permitir o factory reset e troca do idioma via interface gráfica.

1.2.5.31 Reutilização de definições de objetos de rede, hosts, serviços, período de tempo, usuários, grupos, clientes e servers.

1.2.5.32 Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades especificas a ele.

1.2.5.33 Controle de acesso e dispositivos por zoneamento.

1.2.5.34 Integrar com ferramenta de gerenciamento centralizado disponibilizado pelo próprio fabricante.

1.2.5.35 Traps SNMP ou e-mail para notificações do sistema.

1.2.5.36 Suportar envio de informações via Netflow e possuir informações via SNMP;

1.2.5.37 Ter funcionalidade que permita que o administrador manualmente atribua núcleos ("cores") do CPU para uma interface em particular, dessa forma, todo trafego que passar por esta interface, será tratado unicamente pelos núcleos definidos.

1.2.5.38 Possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes.

1.2.6 Especificações de Balanceamento de Carga e Redundância para Múltiplos Provedores de Internet

1.2.6.1 A solução proposta deve suportar o balanceamento de carga e redundância para no mínimo 2 (dois) links de Internet.

1.2.6.2 A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.

1.2.6.3 A solução proposta deve suportar algoritmo "Round Robin" para balanceamento de carga.

1.2.6.4 A solução proposta deve fornecer opções de condições em caso de falha "Failover" do link de Internet através dos protocolos ICMP, TCP e UDP.

1.2.6.5 A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.

1.2.6.6 A solução proposta deve ter ativo/ativo utilizando algoritmo de "Round Robin" e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover).

1.2.6.7 A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6.

1.2.7 Especificações de Alta Disponibilidade

1.2.7.1 A solução proposta deve suportar Alta Disponibilidade (High Availability) ativo/ativo e ativo/passivo.

1.2.7.2 A solução proposta deve notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade.

1.2.7.3 O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.

1.2.7.4 A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.

1.2.7.5 A solução proposta deve suportar sincronização automática e manual entre os firewalls NGFWs em "cluster".

1.2.7.6 A solução deve suportar Alta Disponibilidade (HA) em "Bridge Mode" e Mixed Mode" (Gateway + Bridge).

1.2.8 Especificações do Firewall e roteamento

1.2.8.1 A solução deve ser Standalone Firewall NGFW e com Sistema Operacional fortalecido "Hardening" para aumentar a segurança.

1.2.8.2 A solução proposta deve suportar "Stateful Inspection" baseado no usuário "one-to-one", NAT Dinâmico e PAT.

1.2.8.3 A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall.

1.2.8.4 A solução proposta deve unificar as políticas de ameaças de

forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga baseado na mesma regra do Firewall para facilitar de uso.

1.2.8.5 A solução proposta deve suportar arquitetura de segurança baseado em Zonas.

1.2.8.6 A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e também suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo".

1.2.8.7 A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP.

1.2.8.8 A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).

1.2.8.9 A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.

1.2.8.10 A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.

1.2.8.11 O sistema proposto deve prover mensagem de alertas no Dash Board (Painel de Bordo) quando eventos como, por exemplo: nova firmware disponível para download ou a licença irá expirar em breve.

1.2.8.12 O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI.

1.2.8.13 A solução proposta deve suportar IPv6.

1.2.8.14 A solução proposta deve suportar implementações de IPv6 Dual Stack.

1.2.8.15 A solução proposta deve suportar tuneis 6in4, 6to4, 4in6,6rd.

1.2.8.16 A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.

1.2.8.17 A solução proposta deve suportar DNSv6.

1.2.8.18 A solução proposta deve oferecer proteção DoS contra ataques IPv6.

1.2.8.19 A solução proposta deve oferecer prevenção contra Spoof em IPv6.

1.2.8.20 A solução proposta deve suportar 802.3ad para Link Aggregation.

1.2.8.21 A solução proposta deve suportar 3G UMTS e 4G modem via interface USB para VPN e Link Backup "Plano de Continuidade" - Balanceamento de Carga.

1.2.8.22 A solução proposta deve suportar gerenciamento de banda baseado em Aplicação que permite administradores criarem políticas de banda de utilização de link baseado por aplicação.

1.2.8.23 Flood protection, DoS, DDoS e Portscan.

1.2.8.24 Bloqueio de Países baseados em GeoIP.

1.2.8.25 Suporte a Upstream proxy.

1.2.8.26 Suporte a VLAN DHCP e tagging.

1.2.8.27 Suporte a Multiple bridge.

1.2.8.28 Funcionalidades do portal do usuário.

1.2.8.29 Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).

1.2.8.30 Download dos clientes de autenticação disponibilizados pela ferramenta.

1.2.8.31 Download do cliente VPN SSL em plataformas Windows.

1.2.8.32 Download das configurações SSL em outras plataformas.

1.2.8.33 Informações de hotspot.

1.2.8.34 Autonomia de troca de senha do usuário.

1.2.8.35 Visualização do uso de internet do usuário conectado.

1.2.8.36 Acesso a mensagens em quarentena.

1.2.8.37 Opções base de VPN.

1.2.8.38 Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key.

1.2.8.39 L2TP e PPTP.

1.2.8.40 VPN SSL, IPSEC.

1.2.8.41 Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

1.2.9 Funcionalidades base de QoS e Quotas

1.2.9.1 QoS aplicado a redes e usuários de download/upload em tráfegos baseados em serviços.

1.2.9.2 Otimização em tempo real do protocolo Voip.

1.2.9.3 Suporte a marcação DSCP.

1.2.9.4 Regras associadas por usuário.

1.2.9.5 Criar regras que limitem e garantam upload e download.

1.2.9.6 Permitir criar regra de QoS individualmente e compartilhada.

1.2.10 Filtragem e Segurança Web

1.2.10.1 Proporcionar transparência total de autenticação no proxy, provendo segurança antimalware e filtragem web.

1.2.10.2 Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas agregadas a pelo menos 92

categorias oferecidas pela solução.

1.2.10.3 Realizar autenticação dos usuários nos modos transparente e padrão.

1.2.10.4 As autenticações devem ser feitas via NTLM.

1.2.10.5 Possuir sistema de quotas aplicado por usuários e grupos.

1.2.10.6 Permitir criar políticas por horário aplicado a usuários e grupos.

1.2.10.7 Possuir sistema de malware scanning que realize as seguintes ações:

1.2.10.7.1 Bloquear toda forma de vírus

1.2.10.7.2 Bloquear malwares web

1.2.10.7.3 Prevenir infecção de malwares, trojans e spyware em tráfegos HTTPS, HTTP, FTP e e-mails baseados em acesso web (via navegador).

1.2.10.8 Prover proteção em tempo real de todos os acessos web.

1.2.10.9 A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá manter-se atualizada prevenindo novas ameaças.

1.2.10.10 Prover pelo menos duas engines diferentes de antimalware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.

1.2.10.11 Fornecer Pharming Protection.

1.2.10.12 Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.

1.2.10.13 Permitir criação de regras customizadas baseadas em usuário e hosts.

1.2.10.14 Permitir criar exceções de URLs, usuários e hosts para que não sejam verificados pelo proxy.

1.2.10.15 Validação de certificado.

1.2.10.16 Prover cache de navegação, contribuindo na agilidade dos acessos à internet.

1.2.10.17 Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)

1.2.10.18 Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo.

1.2.10.19 Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.

1.2.10.20 Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.

1.2.10.21 Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais.

1.2.10.22 Especificar um tamanho em Kbytes de arquivos que não devem

ser escaneados pela proteção web.

1.2.10.23 Range aceitável de 1 a 25600KB.

1.2.10.24 Bloquear trafego que não segue os padrões do protocolo HTTP.

1.2.10.25 Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.

1.2.10.26 Nas exceções, permitir definir operadores "AND" e "OR".

1.2.10.27 Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.

1.2.10.28 Permitir definir nas exceções a opção de não realizar escaneamento contra malware.

1.2.10.29 Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas.

1.2.10.30 Permitir criar regras de exceções por endereços IPs de origem.

1.2.10.31 Permitir criar regras de exceções por endereços IPs de destino.

1.2.10.32 Permitir criar exceções por grupo de usuários.

1.2.10.33 Permitir criar exceções por categorias de sites.

1.2.10.34 Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.

1.2.10.35 Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: "Criminal Activities, Finance & Investing, Games and Gambling", entre outras.

1.2.10.36 Permitir editar grupos de categorias pré-estabelecidos pela solução.

1.2.10.37 Deve ter sistema que permita a criação de novas categorias com as seguintes especificações:

1.2.10.37.1 Nome da regra;

1.2.10.37.2 Permitir criar uma descrição para identificação da regra.

1.2.10.37.3 Ter a possibilidade de classificação de pelo menos: Produtivo ou Não produtivo;

1.2.10.37.4 Permitir aplicar Traffic shaping diretamente na categoria.

1.2.10.37.5 Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave.

1.2.10.37.6 Deve permitir importar uma base com domínios e palavras chaves na hora da criação da categoria, a base com informações de domínios e palavras chaves deverá aceitar pelo menos as seguintes extensões: .tar, .gz, .bz, .bz2, e .txt.

1.2.10.37.7 Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro.

1.2.10.38 Ter função para criar grupos de URLs.
1.2.10.39 A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.
1.2.10.40 Permitir ao administrador especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS.
1.2.10.41 Deve permitir que em uma mesma política seja aplicada ações diferentes de acordo com o usuário autenticado.
1.2.10.42 Nas configurações das políticas, deve-se existir pelo menos as opções de: Liberar categoria/URL, bloquear e Alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador.
1.2.10.43 Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.
1.2.10.44 Permitir criar cotas de navegação com os seguintes requisitos:
1.2.10.44.1 Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso.
1.2.11 Controle e Segurança de Aplicações
1.2.11.1 Prover controle para mais de 2600 aplicações diferentes.
1.2.11.2 Controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco.
1.2.11.3 Permitir criar regras de controle por usuário e hosts.
1.2.11.4 Permitir realizar traffic shaping por aplicação e grupo de aplicações.
1.2.11.5 Possibilitar que as regras criadas baseadas em aplicação permitam:
1.2.11.5.1 Bloquear o trafego para as aplicações
1.2.11.5.2 Liberar o trafego para as aplicações
1.2.11.5.3 Criar categorização das aplicações por risco:
1.2.11.5.3.1 Risco muito baixo
1.2.11.5.3.2 Risco baixo
1.2.11.5.3.3 Risco médio
1.2.11.5.3.4 Risco alto
1.2.11.5.3.5 Risco muito alto
1.2.11.6 Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras.
1.2.11.7 Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros.
1.2.11.8 Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post

do Facebook, bloquear o like do Facebook, permitir acesso ao youtube, mas bloquear o upload de vídeos, e etc.

1.2.11.9 Permitir agendar um horário e data específico para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.

1.2.12 Proteção de Redes

1.2.12.1 Prover funcionalidade de Intrusion Prevention System (IPS)

1.2.12.2 Proporcionar alta performance na inspeção dos pacotes

1.2.12.3 Possuir mais de 6500 assinaturas conhecidas.

1.2.12.4 Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.

1.2.12.5 Proporcionar flexibilização na criação das regras de IPS, ou seja, permitir que as regras possam ser aplicadas tanto para usuários quanto para redes, permitindo total customização.

1.2.12.6 Possuir funcionalidade Anti-DoS.

1.2.12.7 Deve-se permitir customizar os valores das seguintes funcionalidades de DoS:

1.2.12.7.1 SYN Flood

1.2.12.7.2 UDP Flood

1.2.12.7.3 TCP Flood

1.2.12.7.4 ICMP Flood

1.2.12.7.5 IP Flood

1.2.12.8 Possuir templates pré-configurados pelo fabricante havendo sugestões de fluxo dos pacotes, exemplo: LAN to DMZ, WAN to LAN, LAN to WAN, WAN to DMZ, e etc.

1.2.12.9 Possuir proteção contra spoofing.

1.2.12.10 Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.

1.2.12.11 Possuir funcionalidade para o administrador poder criar by-pass de DoS.

1.2.12.12 Permitir o administrador clonar templates existentes para ter como base na hora da criação de sua política customizada.

1.2.13 Possuir proteção avançada contra ameaças persistentes (APT)

1.2.13.1 Detectar e bloquear tráfico de pacotes suspeitos e maliciosos que trafegam pela rede onde tentam realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, Firewall e outros.

1.2.13.2 Possuir logs e relatórios que informem todos eventos de APT.

1.2.13.3 Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças

persistentes.

1.2.13.4 Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.

1.2.13.5 Proteção para E-mails

1.2.13.6 Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.

1.2.13.7 Possuir serviço de reputação para monitoramento dos fluxos dos e-mails, sendo assim, o AntiSpam deverá bloquear e-mails considerados com má reputação na internet e pelo fabricante.

1.2.13.8 Bloquear SPAN e MALWARES durante a transação SMTP.

1.2.13.9 Possuir duas engines de antivírus para duplo escaneamento.

1.2.13.10 Ter proteção em tempo real, a solução deverá realizar consultas na nuvem para verificar a integridade e segurança dos e-mails que passam pela solução e assim tomar ações automáticas de segurança caso necessário.

1.2.13.11 Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.

1.2.13.12 Possuir funcionalidade que permite detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo.

1.2.13.13 Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customiza-los de acordo com o desejado.

1.2.13.14 Ter suporte a criptografia TLS para SMTP, POP e IMAP.

1.2.13.15 As ações dos e-mails considerados SPAN devem ser:

1.2.13.15.1 Drop

1.2.13.15.2 Warn

1.2.13.15.3 Quarantine

1.2.13.16 Poder definir um prefixo no subject de cada e-mail considerado SPAM, como por exemplo: [SPAN] Marketing etc. etc. etc.

1.2.13.17 Permitir visualizar os e-mails que se encontram na fila para serem enviadas.

1.2.13.18 Possuir funcionalidade que permita a adição de um banner no final dos E-mails analisados pela solução.

1.2.13.19 Possuir funcionalidade de allowlist e blocklist.

1.2.13.20 Possuir funcionalidade que rejeite e-mails com HELO invalido e/ou que não possuam RDNS.

1.2.13.21 Permitir que o escaneamento seja feito tanto para e-mails de entrada quanto para os de saída.

1.2.13.22 **Quarentena de E-mail**

1.2.13.23 Possuir quarentena para os e-mails e opções de notificações

para o administrador.

1.2.13.24 E-mails que possuem malwares e spam e foram quarentenados, devem ter a opção para serem pesquisados por filtros como: data, sender, recipient e subject, todos eles devem possuir a opção para realização do release da mensagem e a opção para remoção.

1.2.13.25 O usuário deve poder gerenciar sua quarentena de e-mails através de um portal disponibilizado pela própria solução, onde ele poderá visualizar e realizar release das mensagens em quarentena.

1.2.13.26 As regras do administrador não poderão ser ignoradas, o usuário tomará ações somente as quais for permitido.

1.2.13.27 Permitir o administrador agendar diariamente, semanalmente ou mensalmente o envio de relatório de quarentena para todos os usuários.

1.2.13.28 Possuir funcionalidade de criptografia de e-mails e DLP para os dados

1.2.13.29 Possuir funcionalidade de encriptação de e-mails que não necessite a configurações complexas que envolvam certificados entre outros requisitos.

1.2.13.30 Os e-mails criptografados poderão ter seu conteúdo armazenado em um arquivo PDF.

1.2.13.31 Ter como funcionalidade a possibilidade de o usuário poder registrar sua própria senha de segurança para que seja possível abrir os e-mails criptografados.

1.2.13.32 Possuir também funcionalidade para geração de senhas aleatórias para descriptografar o conteúdo.

1.2.13.33 Permitir enviar anexos junto aos e-mails criptografados.

1.2.13.34 Para o usuário final o uso desta criptografia deve ser completamente transparente, ou seja, não se deve utilizar qualquer software adicional, plugin, ou client instalado no equipamento.

1.2.13.35 Possuir funcionalidade de DLP nos E-mails

1.2.13.36 A engine de DLP deve ser automática na hora de escanear os e-mails e anexos, assim identificando todos os dados sensíveis encontrados no e-mail sem qualquer intervenção.

1.2.13.37 Ter a opção de criar exceções individuais para cada tipo de situação.

1.2.13.38 As regras devem corresponder para as redes de origem e alvos específicos como a especificados por URLs.

1.2.13.39 Suporte a operadores lógicos

1.2.13.40 Poder definir tamanho máximo para escaneamento.

1.2.13.41 Permitir bloquear e liberar ranges IP.

1.2.13.42 Suporte para utilização de Wildcards

1.2.13.43 Anexar automaticamente um prefixo/sufixo para autenticação.

1.2.14 Proteção para proteção de servidores WEB (WAF)

1.2.14.1 Possuir funcionalidade de proxy reverso

1.2.14.2 Possuir engine de URL hardening e prevenção a directory traversal.

1.2.14.3 Possuir engine Form hardening.

1.2.14.4 Proteção contra SQL injection

1.2.14.5 Proteção contra Cross-site scripting

1.2.14.6 Possuir duas engines de antivírus disponíveis para análise de malware.

1.2.14.7 Permitir definir o fluxo que o antivírus irá atuar, se será no upload ou download.

1.2.14.8 Permitir limitar o tamanho máximo em que o antivírus irá atuar.

1.2.14.9 Permitir bloquear conteúdo considerado unscannable.

1.2.14.10 Possuir HTTPS (SSL) encryption offloading.

1.2.14.11 Proteção para cookie signing com assinaturas digitais.

1.2.14.12 Possuir Path-based routing.

1.2.14.13 Suporte ao protocolo do Outlook anywhere.

1.2.14.14 Possuir autenticação reversa para acesso aos servidores web.

1.2.14.15 Permitir criar templates de autenticação, onde o administrador poderá configurar uma página em HTML para autenticação.

1.2.14.16 Ter abstração de servidores virtuais e físicos.

1.2.14.17 Proporcionar função de load balance para que os visitantes possam ser jogados para diversos servidores de forma transparente.

1.2.14.18 Permitir definir qual modo o WAF deve operar, tendo como opção modo de monitoramento apenas e modo para rejeitar as conexões consideradas maliciosas.

1.2.14.19 Bloquear clients com má reputação.

1.2.14.20 Bloquear protocolos com anomalias.

1.2.14.21 Limitar número de requisições.

1.2.15 Proteção de Sandbox na nuvem

1.2.15.1 Prover ambiente de Sandbox na nuvem provido pelo próprio fabricante.

1.2.15.2 Realizar inspeções de executáveis e documentos que possuam conteúdo executáveis.

1.2.15.3 Possuir suporte aos principais executáveis Windows como: .exe, .com e .dll.

1.2.15.4 Possuir suporte aos principais documentos do Word como: .doc, .docx, .docm e .rft.

1.2.15.5 Realizar analise em documentos PDF.

1.2.15.6 Realizar analise de qualquer tipo de conteúdo que possua os seguintes tipos de arquivos: ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet

1.2.15.7 Suporte a mais de 20 tipos de arquivos e extensões.

1.2.15.8 Realizar analises dinâmicas de malwares e ameaças, rodando estes arquivos em ambientes reais e em produção, todos providos na nuvem pelo fabricante.

1.2.15.9 Relatórios detalhados das ameaças bem como visibilidade dos alertas na dashboard da solução.

1.2.15.10 O tempo em média das análises devem ser menores do que 120 segundos.

1.2.15.11 Suportar a análise de links de download em tempo real.

1.2.15.12 Permitir escolher pelo menos duas regiões para as quais os arquivos para analise devem ser enviados.

1.2.15.13 Possuir uma opção que permita a solução identificar automaticamente o caminho com menor latência para envio dos arquivos para analisa.

1.2.15.14 Permitir o administrador criar exceções para aqueles eventos que serão considerados falsos positivos.

1.2.15.15 O firewall NGFW deve oferecer relatórios locais referente a todos os eventos registrados pela funcionalidade de Sandbox.

1.2.16 Solução de gerenciamento

1.2.16.1 A solução deverá prover uma ferramenta distribuída pelo mesmo fabricante para gerenciamento centralizado de ambos os firewalls NGFWs adquiridos pela contratante.

1.2.16.2 A solução de gerenciamento deverá permitir que o administrador da ferramenta possa criar políticas de gerenciamento para um ou mais equipamentos e aplica-los todos de uma única vez.

1.2.16.3 As políticas de configurações devem ter no mínimo as seguintes opções:

1.2.16.3.1 Proteção e políticas de acesso web

1.2.16.3.2 Controle de aplicativos

1.2.16.3.3 IPS

1.2.16.3.4 VPN

1.2.16.3.5 E-mail

1.2.16.3.6 Firewall

1.2.16.4 A solução deverá oferecer funcionalidade que permita o administrador criar templates de configuração para que o administrador possa aproveitar as mesmas regras para novos firewalls NGFWs.

1.2.16.5 Deverá haver na dashboard da solução, indicadores que

permitam o administrador avaliar a saúde do equipamento de uma maneira fácil para visualização.

1.2.16.6 Possuir múltiplas formas de customização de warning thresholds.

1.2.16.7 Possuir flexibilização na hora da criação de grupos de firewall NGFWs gerenciados, sendo possível diferencia-los como por exemplo: Região, modelo ou outro parâmetro.

1.2.16.8 Deverá possuir funcionalidade que permita o administrador delegar funções para diferentes técnicos com diferentes funções.

1.2.16.9 Possuir logs de todas as alterações para que seja possível realizar o rollback das alterações realizadas caso necessário.

1.2.17 Ferramenta de relatórios e gestão de logs

1.2.17.1 A ferramenta deve estar hospedada em Data Center com certificação Tier III ou ISO27001 ou SOC 2 Type 2;

1.2.17.2 A CONTRATADA deve disponibilizar no mínimo 500GB líquido para armazenamento de logs;

1.2.17.3 A solução deve suportar no mínimo 250 eventos por segundo ou 10GB de logs por dia;

1.2.17.4 A ferramenta de relatórios deverá suportar no mínimo os seguintes relatórios:

1.2.17.4.1 Ataques detectados;

1.2.17.4.2 Categorias de aplicações mais acessadas;

1.2.17.4.3 Categorias WEB mais acessadas;

1.2.17.4.4 Aplicações WEB mais utilizadas

1.2.17.4.5 Websites mais acessados;

1.2.17.4.6 Usuário ou equipamento com maior consumo de banda;

1.2.17.4.7 Usuário ou equipamento com maior número de sessões;

1.2.17.4.8 Aplicações de Maior Risco;

1.2.17.4.9 Aplicações com maior vulnerabilidade;

1.2.17.4.10 Top Malware, Botnets, Spyware e Adware detectados;

1.2.17.4.11 Usuários ou dispositivos com maior risco;

1.2.17.4.12 Aplicações mais acessadas;

1.2.17.4.13 Redes sociais mais acessadas;

1.2.17.4.14 Aplicações de streaming de áudio e vídeo mais acessadas;

1.2.17.4.15 Aplicações P2P mais acessadas;

1.2.17.4.16 Aplicações de Game mais acessadas;

1.2.17.5 Permitir a personalização dos relatórios padrão da solução, permitindo o administrador criar relatórios de acordo com as necessidades do ambiente e informações desejadas.

1.2.17.6 Permitir que o administrador realize agendamentos destes relatórios para que estes sejam enviados via e-mail para todos os e-mails

cadastrados.

1.2.17.7 Ter fácil identificação das atividades de rede e ataques em potencial.

1.2.17.8 Armazenar histórico dos relatórios em disco local.

1.2.17.9 Possuir relatórios únicos para cada um dos módulos ofertados pela solução.

1.2.17.10 Possuir múltiplos formatos de relatório, pelo menos tabular e gráfico.

1.2.17.11 Permitir exportar relatórios para: PDF, Excel e HTML.

1.2.17.12 Possuir relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing, Wikipédia e Google.

1.2.17.13 Possuir relatórios que informem principais atividades em cada módulo.

1.2.17.14 Ter logs em tempo real.

1.2.17.15 Ter logs arquivados para consulta posterior.

1.2.17.16 Permitir que o administrador consiga realizar pesquisas dentro dos logs arquivados.

1.2.17.17 Possuir logs de auditoria.

1.2.17.18 Ter sua gerência totalmente baseada em acesso web.

1.2.17.19 Permitir que o administrador crie regras baseadas em usuários onde cada usuário criado poderá ter acesso a funcionalidades especificas na ferramenta.

1.2.17.20 Possuir no mínimo 2 (duas) dashboard sendo uma exclusiva para os relatórios e outra exclusiva para visualização da saúde do equipamento (CPU e memória).

1.2.17.21 O administrador deve poder acessar estes relatórios de qualquer lugar através de apenas um navegador.

1.2.17.22 Ter total gerência sobre a retenção dos dados armazenados neste equipamento.

1.2.17.23 Ter disponibilidade em firewall NGFW virtual e software caso necessário instalar o firewall NGFW em um hardware baseado em Intel.

2. <u>ITEM 2: Serviço de Proteção para Estações de Trabalho e Servidores</u>

2.1. A solução deve ser licenciada para todo o parque de TIC da FEMA, ou seja, para 300 (trezentos) dispositivos, servidores ou estações de trabalho.

2.2. Será de responsabilidade da contratada administrar e suportar a solução de proteção, garantido o pleno funcionamento do serviço.

2.3. Console de Gerenciamento

2.3.1. O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um

único fornecedor;

2.3.2. O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS);

2.3.3. O acesso ao Console deve suportar várias sessões simultâneas;

2.3.4. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;

2.3.5. Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor;

2.3.6. Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;

2.3.7. O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes sistemas operacionais em todas as versões/distribuições/releases:

2.3.7.1. Microsoft Windows 10

2.3.7.2. Microsoft Windows Server 2012, 2012 R2, 2016 e 2019;

2.3.7.3. Ubuntu Server e Desktop 12.04, 14.04, 16.04.1 e 18.04.1;

2.3.7.4. CentOS 6 e 7;

2.3.7.5. Debian 7, 8 e 9;

2.3.7.6. Fedora 19, 20, 23 e 29;

2.3.8. O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE;

2.3.9. Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores;

2.3.10. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

2.3.11. Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo;

2.3.12. Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso);

2.3.13. Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.

2.3.14. Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento;

2.3.15. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;
2.3.16. A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente;
2.3.17. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador);
2.3.18. O log deve ser centralizado e conter, no mínimo, os seguintes itens:
2.3.18.1. Nome da ameaça
2.3.18.2. Nome do arquivo infectado
2.3.18.3. Data e hora da infecção
2.3.18.4. Ação tomada
2.3.18.5. Endereço IP da máquina
2.3.18.6. Usuário autenticado na máquina
2.3.18.7. Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado via rede;
2.3.19. O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques;
2.3.20. Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.

2.4. Atualização de Vacinas

2.4.1. Atualização incremental e on-line das vacinas;
2.4.2. Atualização em clientes móveis (notebook, laptop, netbook, ultrabook, e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador;
2.4.3. Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet;
2.4.4. Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante;
2.4.5. Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função;
2.4.6. Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução;

2.4.7. Qualquer atualização deve ser possível sem a necessidade de reinicialização do computador ou serviço para aplicá-la;
2.4.8. Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;
2.4.9. O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.

2.5. Cliente Gerenciado

2.5.1. A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits;
2.5.2. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação com os seguintes sistemas operacionais em todas as versões/distribuições/releases:
2.5.2.1. Microsoft Windows XP SP3, Vista, 7, 8, 8.1, 10;
2.5.2.2. Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019;
2.5.2.3. Ubuntu Server e Desktop 12.04, 14.04, 16.04.1 e 18.04.1;
2.5.2.4. CentOS 5, 6 e 7;
2.5.2.5. Debian 7, 8 e 9;
2.5.2.6. Fedora 19, 20, 23 e 29;
2.5.3. O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede;
2.5.4. O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento;
2.5.5. Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante;
2.5.6. Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento;
2.5.7. Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária;
2.5.8. O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas (*locked*) através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.

2.6. Funcionalidade de Firewall e Sistema de Prevenção de Intrusão (IPS)

2.6.1. A funcionalidade deve suportar os protocolos TCP e UDP;
2.6.2. Reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio;

2.6.3. Possuir proteção contra-ataques de *Denial of Service (DoS), Port-Scan* e *Spoofing e botnet*;
2.6.4. Possibilidades de criação de assinaturas personalizadas para detecção;
2.6.5. Possibilidade de agendar a ativação de novas regras do *firewall*;
2.6.6. Possibilidade de criar regras diferenciadas por aplicações;
2.6.7. todos os executáveis da lista ou liberar somente os executáveis da lista;
2.6.8. Bloqueio de ataques baseado na exploração da vulnerabilidade;
2.6.9. Permitir integração com navegadores WEB para prevenção de ataques;
2.6.10. Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.

2.7. Funcionalidade de Antimalware

2.7.1. A solução deve prover proteção em tempo real contra vírus, *trojans*, *worms*, spyware, *adwares* e outros tipos de códigos maliciosos;
2.7.2. As configurações do antimalware deverão ser realizadas através da mesma console de todos os itens da solução;
2.7.3. Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real);
2.7.4. Permitir verificação das ameaças de maneira manual, agendada e em Tempo-Real detectando ameaças no nível do Kernel do Sistema Operacional fornecendo a possibilidade de detecção de Rootkits;
2.7.5. Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com intervalos de tempo determinados, de forma a reduzir impacto em ambientes;
2.7.6. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar;
2.7.7. Verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook, ou que utilizem os protocolos POP3/SMTP;
2.7.8. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados;
2.7.9. Deve suportar varredura de, no mínimo, os seguintes padrões de compactação:
2.7.9.1. CAB;
2.7.9.2. ZIP;
2.7.9.3. RAR;
2.7.9.4. LHA;
2.7.9.5. ARJ;

2.7.9.6. TAR;

2.7.10. Capacidade de terminar o processo e serviço da ameaça no momento de detecção;

2.7.11. Capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede;

2.7.12. Possibilidade de bloquear verificação de malware em recursos mapeados da rede;

2.7.13. Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos;

2.7.14. Não serão aceitas soluções de Antimalware que possuam engine de terceiros;

2.7.15. Permitir o bloqueio da execução de aplicações baseado em nome e pasta.

2.8. Funcionalidade de Reconhecimento de Novas Ameaças

2.8.1. A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;

2.8.2. Capacidade de detecção de *keyloggers* por comportamento dos processos em memória;

2.8.3. Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts;

2.8.4. Capacidade de detecção de *Trojans* e *Worms* por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção;

2.8.5. Possibilidade de agendar a varredura da detecção de novas ameaças.

2.8.6. Uso de sandboxing na nuvem para analisar o comportamento de malwares, com SLA de 5 minutos até 1 hora de resposta.

2.9. Funcionalidade de Controle de Dispositivos

2.9.1. Controlar o uso de dispositivos com comunicação infravermelha, *firewire*, portas seriais e paralelas, através de mecanismos de permissão e bloqueio, identificando-os pelo "Class ID" e pelo "Device ID";

2.9.2. Permitir criar políticas de bloqueio de dispositivos distintas para diferentes grupos da base de estações conectadas;

2.9.3. Gerenciamento integrado à console de gerência da solução.

2.9.4. A solução deve ser capaz de permitir ou negar o uso dos dispositivos com base nos seguintes critérios:

2.9.4.1. Fabricante

2.9.4.2. Modelo
2.9.4.3. Número de Série

2.10. Funcionalidade de Controle WEB

2.10.1. Controlar acesso a sites, possibilitando o bloqueio do mesmo;
2.10.2. Permitir criar políticas de bloqueio com base em categorias e lista de URL;
2.10.3. Permitir gerar relatórios de sites acessados e bloqueados;

2.11. Relatórios e Monitoramento

2.11.1. Gerar, no mínimo, os relatórios abaixo descritos, tanto de maneira gráfica quanto em arquivos CSV, PDF, HTML ou MHTML, permitindo escolher o período de consulta desejado:
2.11.1.1. Listagem dos malwares que infectaram determinada máquina;
2.11.1.2. Listagem das máquinas que estão infectadas por determinado *malware*;
2.11.1.3. Relatório dos totais de códigos maliciosos detectados, indicando aqueles de maior incidência;
2.11.1.4. Listagem das máquinas nas quais o antimalware deixou de remover algum código malicioso;
2.11.1.5. Número total de arquivos maliciosos removidos;
2.11.1.6. Relatório de máquinas cuja atualização de componentes do software antimalware e assinaturas não foi realizada, incluindo a data da última atualização;
2.11.1.7. Relatório de máquinas com maior número de infecções;
2.11.1.8. Relatório de atualização de componentes do software antimalware e assinaturas;
2.11.1.9. Relatório das máquinas que não se comunicaram com o servidor de antimalware a partir de uma determinada data.;
2.11.1.10. Possibilidade de exibir a lista de servidores e estações que possuam o antimalware instalado, contendo informações como nome da máquina, usuário autenticado, versão do *engine*, data da vacina, data da última verificação e status;
2.11.1.11. Sumário de eventos IPS por assinatura, por alvo, por endereço IP de origem, principais nós atacados, principais assinaturas;
2.11.2. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento.
2.11.3. Deverá ter um console de administração de licenças em nuvem, de onde é possível revisar os detalhes de equipamentos aos quais foram provisionados o licenciamento.

2.12. Funcionalidades Tecnológicas

2.12.1. A console deverá funcionar também através de um Appliance

Virtual.

2.12.2. Dentro do módulo de firewall deverá possuir a funcionalidade de bloqueio de exploits.

2.12.3. Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.

2.12.4. Deverá contar com um filtro de correio para a detecção de malware e spam.

2.12.5. Deverá ser uma solução que pode ser utilizada e administrada através de um console de administração remota de antivírus para os sistemas operacionais Windows, Linux e Mac.

2.12.6. A solução Anti Malware deverá contar com a tecnologia HIPS (Host-based Intrusion Prevention System) para proteger a manipulação indevida e detectar ameaças com base na conduta do host.

2.12.7. O produto deverá ter um controle web para limitar o acesso a sites web por categoria, além de poder mostrar ao usuário uma notificação de bloqueio.

2.12.8. Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.

2.12.9. O firewall do produto deverá ser bidirecional, assim como detectar as redes seguras.

2.12.10. A solução deverá realizar exploração em estado inativo para poder fornecer desta forma uma proteção pró ativa enquanto o equipamento não está em uso.

2.12.11. A console de administração deverá ter um Appliance Virtual aberto para instalar e utilizar em ambientes virtuais, para ter um ambiente distribuído e de fácil instalação.

2.12.12. O acesso ao console de administração do antivírus deve ser feito com duplo fator de autenticação integrado dentro da mesma console aonde é possível ativa-lo se a necessidade de nenhum add-on adicional.

2.12.13. O console de administração de licenças deve ser na nuvem, aonde é possível revisar os detalhes dos equipamentos que estão utilizando a licença do antivírus.

2.12.14. A versão mais atual do antivírus deve ter proteção a equipamentos com sistemas operacionais Windows XP.

2.12.15. A console de administração deverá suportar a instalação em ambiente com sistema operacional Linux.

2.12.16. Detecção do malware por DNA do vírus.

2.12.17. Deverá ter a capacidade de atualizar os patches do sistema operacional.

2.12.18. A solução deve ser capaz de definir uma lista de usuários específicos que podem fazer utilização dos dispositivos. Para dispositivos de armazenamento a solução deve permitir a configuração das seguintes permissões: Leitura e Escrita, Bloqueio, Somente Leitura e Advertência.

2.12.19. Quando se conectar ou utilizar um dispositivo de armazenamento a solução de antivírus deve proporcionar as seguintes opções: Escancear, Não realizar nenhuma ação e Se lembrar dessas ações.

2.12.20. Deverá permitir a execução remota de scripts, arquivos batches e pacotes personalizados através da console.

2.12.21. Deve permitir gerar grupos de clientes dinâmicos e grupos estáticos.

2.12.22. O fabricante deverá proporcionar ao menos três formas diferentes de realizar a instalação do console de administração remota: Instalação Tudo em Um, Instalação por Componentes e em Appliance Virtual.

2.12.23. O Appliance Virtual deverá suportar ao menos as seguintes plataformas de virtualização: VMWare vSphere, Oracle Virtual Box, Microsoft Hyper-V e Azure.

2.12.24. A console de administração deverá suportar a instalação em Linux.

2.12.25. Deve contar com desinstalador de antivírus de terceiros.

2.12.26. A solução de proteção Antispam deve realizar as verificações utilizando o protocolo SSL.

2.12.27. A solução antivírus deve contar um Firewall pessoal com os seguintes modos de configuração: Modo automático, Modo Interativo, Modo baseado em políticas e Modo de Aprendizagem.

2.12.28. O fabricante deverá ter suporte local em idioma português.

2.12.29. O fabricante deverá ter documentação publicada na internet no idioma português.

2.12.30. Possuir proteção contra ransomware, com um módulo específico, utilizando a console para configuração e distribuição de políticas aos endpoints.

2.12.31. Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push (EPNS).

2.12.32. Funcionalidade de Inventário de Hardware (CPU, RAM, Armazenamento, Versão de Sistema Operacional e Periféricos conectados)

2.12.33. Possuir no mínimo 31 modelos de relatórios pré configurados com filtros e conjuntos de filtros na console de gerenciamento.

2.13. Quarentena do Correio Eletrônico

2.13.1. Mensagens de e-mail de spam e de quarentena podem ser

armazenadas em um sistema de arquivos local, não no banco de dados de caixa de correio do Exchange.

2.13.2. A criptografia e a compactação de arquivos de e-mail em quarentena devem ser armazenadas localmente.

2.13.3. Arquivos de email em quarentena excluídos podem ser restaurados usando a interface de linha de comando do produto do fabricante do produto de proteção de email (desde que eles ainda não tenham sido excluídos do sistema de arquivos).

2.13.4. Os relatórios de quarentena devem ser enviados para um endereço de email especificado usando uma tarefa agendada.

2.13.5. É possível armazenar mensagens de destinatários inexistentes: aplica-se a mensagens marcadas para serem colocadas em quarentena por proteção antivírus, proteção antispam ou regras.

2.13.6. O administrador da Quarentena de e-mail deve estar disponível nos três tipos de quarentena: Quarentena local, Correio electrônico de quarentena e Quarentena de MS Exchange

2.13.7. Deve ter uma interface da Web da Quarentena da Web.

2.13.8. Deve ter validação de mensagem com SPF, DKIM e DMARC, localmente no mesmo servidor de email no aplicativo de proteção de email.

2.13.9. Para verificar o banco de dados por demanda, deve usar a API do EWS (Serviços Web do Exchange) para se conectar ao Microsoft Exchange Server usando HTTP / HTTPS.

2.13.10. A proteção de email deve ter a possibilidade de instalar por componentes, você pode escolher os componentes para adicionar ou remover.

2.13.11. O produto de segurança deve ter uma interface de linha de comando que ofereça aos usuários e administradores avançados opções mais profundas para gerenciar o produto.

2.13.12. As regras de correio devem ser classificadas em três níveis e avaliadas na seguinte ordem:

2.13.12.1. Regras de filtragem: regra avaliada antes do antispam e da verificação antivírus

2.13.12.2. Regras de processamento de anexos: regra avaliada durante a verificação antivírus

2.13.12.3. Regras de processamento de anexos: regra avaliada durante a verificação antivírus

2.13.13. Deve poder explorar mensagens de conexões autenticadas ou internas.

2.13.14. A solução deve ser capaz de excluir o cabeçalho SCL existente antes da verificação e pode ser desativada se for necessário manter o

cabeçalho do nível de confiança em relação ao spam.

2.14. Regras

2.14.1. Deve-se poder excluir o anexo de uma mensagem no Transporte de Email, no banco de dados da caixa de correio e na verificação do banco de dados.

2.14.2. Deve-se poder adicionar uma string personalizada ao campo de cabeçalho (ao cabeçalho da mensagem).

2.14.3. Deve ser possível adicionar várias ações para uma regra.

2.15. Condições

2.15.1. Deve-se poder aplicar a mensagens enviadas a um destinatário validado no Active Directory sobre proteção de transporte de email.

2.15.2. Deve-se poder aplicar condições a mensagens que tenham anexos com nomes específicos.

2.15.3. Deve-se poder aplicar condições a mensagens de um remetente com um domínio específico no endereço de e-mail.

2.15.4. Deve ser possível analisar se a mensagem contém um arquivo danificado na proteção de transporte de email e na proteção de banco de dados da caixa de entrada de email.

2.15.5. O produto deve suportar múltiplas funções Microsoft Exchange Server 2007, 2010 e Windows SM 2008 e 2011, proteção contra spam, regras, sobre proteção de transporte de e-mail, varredura de banco de dados sob demanda, proteção de banco de dados dos dados da caixa de correio e da quarentena.

2.15.6. O produto deve suportar borda e caixa de correio, Windows Exchange Server 2016, proteção contra spam, regras, proteção de transporte de email, verificação de banco de dados sob demanda e quarentena de email.

3. <u>ITEM 03: Serviço de Suporte Técnico e Monitoramento de Infraestrutura</u>

3.1. Para garantir a continuidade e qualidade dos serviços ofertados neste lote e do ambiente atual de infraestrutura da contratante, devem ser monitorados e suportado pela contratada.

3.2. <u>Sobre Chamados e Atendimento Técnico</u>

3.2.1. A contratante poderá abrir chamados de manutenção através de chamada telefônica para número fixo, central de atendimento via navegador (WEB) ou correio eletrônico sem a necessidade prévia consulta e/ou qualquer liberação por parte da contratada;

3.2.2. O atendimento técnico presencial deverá ocorrer de segunda a sexta-feira (exceto feriados) das 09:00h às 18:00h, sob demanda;

3.2.3. O atendimento técnico remoto deverá ocorrer de segunda a sexta-feira (exceto feriados) das 08:00h às 18:00h;

3.2.4. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas de hardware e/ou software;

3.2.5. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos;

3.2.6. A empresa Contratada se responsabilizará pelas despesas com material de escritório, reprodução de documentos (fotocopias, etc), mídias de armazenamento de dados e materiais diversos, que forem necessários à execução dos serviços de manutenção dos serviços e pelos seus profissionais;

3.2.7. A contratada deverá realizar atendimentos remotos à equipe de tecnologia da informação da contratante, a partir de solicitações recebidas dos técnicos ou gestores de contrato da contratante via sistema de atendimento, telefone ou correio eletrônico;

3.2.8. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados;

3.2.9. Correlacionar incidentes a fim de identificar sua causa-raiz, solucioná-la e prevenir novas ocorrências;

3.2.10. Executar ações correlatas, que demandem maior esforço ou complexidade (ex: instalações e ou atualizações de software em grande quantidade de equipamentos, elaboração de roteiro específico, etc.), solicitadas diretamente pelo Gestor do Contrato por parte da Contratante e devidamente registradas no Sistema de atendimento técnico;

3.2.11. Deverá realizar configurações solicitadas pela contratante, tais como: regras de trafego de dados, rotas, políticas e demais configurações especificas dos componentes da solução;

3.2.12. Planejamento e aplicação de atualizações e ou correções de firmware com programação prévia de forma que não seja gerado nenhum tipo de indisponibilidade ou a mínima possível acordada com a contratante;

3.2.13. Realização de otimizações nas configurações para melhora do desempenho, quando observadas quedas de desempenho ou indisponibilidades pela Contratante;

3.2.14. Na impossibilidade de resolução de problema técnico telefônico ou acesso remoto a contratada deverá disponibilizar uma visita presencial para avaliação e resolução do problema;

3.2.15. Deverá atualizar os softwares da solução sempre que disponíveis e homologados pelo fabricante. Acordando e alinhando as operações com a contratante;

3.2.16. A contratada deverá garantir que os profissionais designados

para atendimento técnico serão capacitados;

3.2.17. Todo acesso remoto à rede da contratante, deve ser feito via VPN cliente-to-site;

3.2.18. O meto de autenticação remota na rede dever possuir duplo fator de autenticação, através de aplicativo mobile (iOS, Android), autenticação via Push, hard tokens, scripts em PowerShell e SMS;

3.3. Garantia de Tempo de Resposta e Nível de Serviço

3.3.1. A garantia de tempo de resposta será realizada conforme critérios de prioridades a seguir:

Classe	Descrição	Inicio do atendimento em até:
1	Serviço indisponível	30 minutos
2	Suporte técnico de maior impacto	4 horas
3	Suporte técnico com menor impacto	8 horas
4	Manutenção preventiva	Programada

3.3.2. O acordo de nível de serviço para suporte técnico deverá obedecer ao seguinte escopo:

Prioridade	Descrição
1 (Emergencial)	O serviço está for a de operação ou há um impacto crítico nas operações dos negócios.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações de negócio sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	O desempenho operacional do serviço está prejudicado, não causando quebra de funcionamento ou de operação.

3.4.1 As horas para primeiro atendimento e resolução de incidentes são horas úteis e serão contabilizadas dentro do horário de atendimento descrito neste termo de referência.

3.5 Central de Chamados e Informações

3.5.1 A contratada deverá disponibilizar e gerenciar os atendimentos técnicas da contratante através de portal de gerenciamento de atendimentos com acesso através de navegador web;

3.5.2 Mesmo os chamados sendo abertos através de ligação telefônica ou

correio eletrônico, os chamados deverão ser registrados na central;

3.5.3 A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições;

3.5.4 A contratada deverá emitir relatórios mensais abrangendo, no mínimo, requisições, incidentes, informações de atendimentos e soluções conforme linha de atendimento com especificações e detalhes de cada atendimento;

3.5.5 A contratante deverá ser avisada através de e-mail sobre a abertura e solução de qualquer tipo de solicitação através do portal WEB, telefone e e-mail;

3.5.6 O sistema operacional e servidor responsável por suportar a console de gerenciamento de atendimentos e informações fica sob responsabilidade da contratada, sendo essa responsável por sua atualização e manutenção;

3.5.7 A solução deverá conter a possibilidade de criação de regras de negócio, para automação no atendimento técnico especializado;

3.5.8 O sistema de gerenciamento de chamados deverá ter histórico de alterações do chamado bem como solução, para eventuais processos de auditoria;

3.5.9 A solução de atendimento e informações deverá constar com a possibilidade de cadastro e organização de ativos de rede, tais como: Firewall, Switches, dispositivos de rede e demais itens com acesso à rede;

3.5.10 A contratada deverá garantir que a solução de atendimento e informações conte com uma área de cadastro de contatos, para consulta pela contratante;

3.5.11 Deverá ser possível anexar documentos de qualquer tipo na abertura e gerenciamento de atendimentos técnicos;

3.5.12 Os atendimentos técnicos deverão ser organizados por categoria, que serão acordados junto a contratante;

3.5.13 O sistema de atendimento deverá contar com a função de aprovação dos atendimentos técnicos, sendo possível o envio de tal aprovação para gestores e responsáveis pelos devidos atendimentos junto a contratante;

3.5.14 Deverá ser possível o envio de notificação de abertura e solução de atendimentos para um grupo de e-mails;

3.5.15 A solução deverá conter módulo que possibilite o inventário de racks dentro do data center;

3.5.16 Os itens de inventario da solução deverão permitir ser anexados aos atendimentos técnicos, criando assim uma relação de atendimento versus dispositivo da contratante;

3.5.17 A solução de atendimento técnico deverá permitir que o chamado possa ser exportado para o formato ".PDF";

3.5.18 A contratada deverá garantir que a solução de atendimento e informações tenha a possibilidade de cadastrar e organizar certificados digitais da contratante;
3.5.19 A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura;
3.5.20 Deverá ser possível a criação de grupos de usuários na solução;
3.5.21 A solução disponibilizada pela contratada deverá ter a possibilidade da criação de várias entidades dentro de um mesmo banco de dados da solução.

3.6 Monitoramento do Ambiente

3.6.1 A contratada deverá monitorar no mínimo 150 sensores ou itens, do ambiente de data center, infraestrutura de rede e equipamentos adquiridos neste documento;
3.6.2 A contratada deverá prover a solução de monitoramento como serviço, pelo prazo de 24 (vinte e quatro) meses;
3.6.3 A disponibilidade e monitoramento deverá ocorrer por 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana;
3.6.4 Deverá ter SLA de disponibilidade da console de gerenciamento de no mínimo 99,98%;
3.6.5 A solução de monitoramento deverá estar hospedada em datacenter com a classificação mínima de Tier III ;
3.6.6 A solução de monitoramento deverá ter portal de acesso de visualização WEB disponibilizada para a contratante;
3.6.7 Deverá ser capaz de enviar alertas de alteração de status de sensores através de correio eletrônico;
3.6.8 Ser capaz de executar áudio pré-definido em caso de alteração de sensores de monitoramento;
3.6.9 Possuir pelo menos os seguintes status para os sensores de monitoramento: Estado normal, estado de alerta e estado de erro;
3.6.10 Possuir a possibilidade para criação de interface WEB com mapa de distribuição de arquitetura com o monitoramento, podendo ter acesso público e/ou autenticado através de contas de usuários internas da solução de monitoramento;
3.6.11 O monitoramento deverá ser compatível com os principais serviços de nuvem pública;
3.6.12 O sistema de monitoramento deverá contar com aplicativo de administração instalável para o sistema operacional Microsoft Windows;
3.6.13 A solução deverá ser compatível com os seguintes protocolos:
3.6.13.1 SNMPv1;
3.6.13.2 SNMPv2;

3.6.13.3 SNMPv3;
3.6.13.4 WMI;
3.6.13.5 SSH;
3.6.14 Deverá ter intervalo mínimo de verificação de 30 (trinta) segundos para os sensores monitorados;
3.6.15 A solução deverá alertar sobre medições incomuns de sensores do ambiente, ou seja, deverá analisar padrões alertando quando houver um estado incomum no monitoramento;
3.6.16 Fornecer informações sobre interrupções ou inoperâncias por meio de cores e/ou formato de ícones, informando se os elementos estão ou não ativos, e se os paramentos estão ou não dentro dos limites preestabelecidos;
3.6.17 Deve permitir o monitoramento da performance com detecção de gargalos e outros problemas da rede, incluindo aqueles relacionados com carga de CPU, uso da memória, utilização de banda, status operacional de interface de rede, tempo de resposta dos dispositivos e eventos de erros;
3.6.18 Possuir um centro de mensagens único para todos os alertas de eventos em dispositivos e/ou serviços de maneira a permitir correlação desses eventos;
3.6.19 Permitir a configuração ou agendamento de descobrimento automático na rede;
3.6.20 Permitir a criação de relatórios de rede personalizados que possam ser exportados para pdf., impresso ou visualizado via HTTP;
3.6.21 Deve suportar IPV4 e IPV6;
3.6.22 Deve permitir interação na configuração do dispositivo através de SNMP v1, v2 e v3;
3.6.23 A solução de monitoramento deverá armazenar dados históricos armazenados em seu banco de dados interno pelo período de 90 (noventa dias);
3.6.24 A solução deverá permitir a personalização de disparadores para sensores, tais como: intervalo de tempo de monitoramento, intervalo de tempo entre erros e alertas e quantidade de alertas consecutivos;
3.6.25 Deverá ser capaz de efetuar detecções automáticas no ambiente da contratante;
3.6.26 A solução de monitoramento deverá ser capaz de entregar e-mails utilizando Relay autenticado;
3.6.27 Deverá ser possível o monitoramento de todas as portas das soluções (hardware) deste termo de referência, mostrando através de tabela de dados e gráficos sua disponibilidade e largura de banda com o intervalo mínimo de 30 (trinta) segundos;
3.6.28 A solução deverá monitorar características físicas das soluções

(hardware) desta solução, tais como: temperatura do hardware, utilização de memória volátil, utilização de armazenamento, utilização e processamento e carga total do equipamento;

3.6.29 Deverá ter sensor com a informação de quantidade de tempo ligado dos equipamentos (hardwares) das soluções;

3.6.30 A solução de monitoramento deverá abrir chamado de maneira automática junto a contratante, após a alteração de um sensor para o estado de alerta ou erro;

3.6.31 Deverá ser possível a geração de relatórios com dados de tabela e gráficos para quaisquer sensores que compõem a solução;

3.6.32 Deverá ser possível a criação de templates de relatórios de monitoramento;

3.6.33 A solução deverá conter sensor de "*Sniffing de Pacotes*" para monitoramento de tráfego incluindo: tráfego por porta e endereço IP, tráfego total, tráfego web (http/https), tráfego de e-mail (IMAP/POP/SMTP), tráfego de transferência de arquivos (FTP e P2P), tráfego de infraestrutura (DHCP, DNS, ICMP e SNMP) e tráfego de acesso remoto (RDP, SSH e VNC);

3.6.34 Deverá suportar monitoramento de tráfego sFlow e Netflow;

3.6.35 Deverá suportar monitoramento nativo de firewall incluindo: status, tráfego inbond e outbound para LAN e WLAN, eventos, atualizações, protocolos mais utilizados (Netflow) e conexões mais utilizadas (Netflow);

3.6.36 Deverá suportar o monitoramento da LAN, WAN e VPNs através de de SNMP, sFLOW, Netflow, Ping e Packet Sniffing;

3.6.37 Deverá suportar o monitoramento da rede WLAN incluindo: Tráfego, intensidade do sinal, status dos dispositivos e último acesso;

3.6.38 Deverá suportar o monitoramento dos seguintes Sistemas Operacionais: Microsoft Windows, Linux e MAC OS X

3.6.39 Deverá suportar o monitoramento das seguintes aplicações: Microsoft Active Directory, SQL Server, Hyper-V e VMWare

3.6.40 Deverá ser capaz de detectar automaticamente sobrecargas de largura de banda em equipamentos de rede gerenciáveis;

3.6.41 A solução deverá ser capaz de monitorar a qualidade de serviço da rede incluindo: jitter, QoS, latência, perda de pacotes, e MOS (mean opinion score);

3.6.42 Deverá ser capaz de monitorar a latência de um dispositivo;

3.6.43 A solução deverá ser capaz de importar arquivos ".MIB", interpreta-los e integra-los ao sistema de monitoramento;

3.7 Relatórios

3.7.1 Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, com:

3.7.2 *Relatório de Chamados (referente ao serviço descrito nesse lote):*

3.7.2.1 Categoria do chamado;

3.7.2.2 Usuário;

3.7.2.3 Ativos relacionados;

3.7.2.4 Data de abertura e fechamento;

3.7.2.5 Status;

3.7.3 *Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote):*

3.7.3.1 Disponibilidade;

3.7.3.2 Consumo de hardware (CPU, memória, disco, consumo de banda);

3.7.3.3 Alertas e erros;

3.7.4 *Relatório de Segurança da Informação mensal:*

3.7.4.1 Ataques detectados;

3.7.4.2 Categorias de aplicações mais acessadas;

3.7.4.3 Categorias WEB mais acessadas;

3.7.4.4 Categorias WEB mais bloqueados;

3.7.4.5 Aplicações WEB mais utilizadas;

3.7.4.6 Aplicações WEB mais bloqueadas;

3.7.4.7 Websites mais acessados;

3.7.4.8 Usuário ou equipamento com maior consumo de banda;

3.7.4.9 Aplicações de Maior Risco;

3.7.4.10 Usuários ou dispositivos com maior risco;

3.7.4.11 Consumo de banda da rede interna;

3.7.4.12 *Relatório de vulnerabilidade trimestral:*

3.7.4.13 Detectar vulnerabilidades em aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

3.7.4.14 Verificar vulnerabilidades em ambiente Windows para, no mínimo: detecção de hot fixes, service packs, registros, peer to peer, portas de serviço habilitadas e antivírus;

3.7.4.15 Detectar vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

3.7.4.16 Efetua descoberta das vulnerabilidades para os equipamentos, produtos, peças ou softwares alocados para atender aos requisitos de todos os itens de serviço e para todo o ambiente computacional da universidade;

3.7.4.17 Apresentar os passos necessários para a realização da remediação das vulnerabilidades encontradas;

3.7.4.18 Scanner (varredura) de rede para identificar portas TCP/UDP

abertas.

3.7.4.19 Riscos baseados na pontuação CVE (Common Vulnerabilities and Exposures);

3.7.4.20 Gerar relatório nos formatos XML, PDF, CSVe HTML;

3.7.4.21 Visualização de problemas por categoria;

3.7.4.22 Cinco níveis de severidade: Critical, High, Medium, Low, Info;

3.7.5 Os relatórios devem serem entregues mensalmente ao gestor do contrato, na data combinada, de forma eletrônica ou em reunião presencial.

3.8 Serviços de Instalação e Configuração

3.8.1 Esse item refere a toda instalação e configuração necessárias para efetuar a prestação de todos os serviços descritos nesse termo de referência.

3.8.2 A contratada deverá instalar e configurar os equipamentos alocados de forma físicas e lógicas seguindo os padrões e melhores práticas recomendadas na norma NBR ISO/IEC 27002 e conforme critérios definidos pela contratante;

3.8.3 Manter durante o período de serviço de instalação e configuração todas as condições de habilitação e qualificação exigidas;

3.8.4 Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

3.8.5 Prestar todos os esclarecimentos que lhe forem solicitados pelo contratante, atendendo prontamente a quaisquer reclamações;

3.8.6 Fornecer toda a mão-de-obra necessária à completa execução do serviço, bem como ferramentas e equipamentos a serem utilizados na manutenção e reparos;

3.8.7 Fornecer e substituir, em caso de necessidade, as peças defeituosas de todos os equipamentos fornecidos como serviço e efetuar os necessários ajustes sem ônus para o contratante desde que os danos causados não sejam de responsabilidade do contratante;

3.8.8 Instalação física de todos os equipamentos em Rack disponibilizado pela Contratante;

3.8.9 Os equipamentos devem estar com firmware e/ou software na versão mais recente e estável recomentada pelo fabricante da solução;

3.8.10 Características especificas do item 1:

3.8.10.1 Os equipamentos devem ser configurados em alta disponibilidade, no modo Ativo-Passivo, um equipamento disponível (configurado), para em caso de falha do equipamento Ativo, o Passivo assuma da operação automaticamente, sem a necessidade de intervenção;

3.8.10.2 A contratada deverá migrar ou executar configurações similares as configurações atuais implementadas no ambiente atual da contratante;

3.8.10.3 Em caso necessite de parada no ambiente, para efetuar a instalação do serviço, deverá ser acordado com a contratante antecipadamente;

3.8.11 Características especificas do item 4:

3.8.11.1 A contratada deve disponibilizar os recursos através de máquinas virtuais, com a quantidade de recurso e sistema operacional solicitado pela contratante.

3.8.12 A contrata deverá elaborar um plano de implementação junto a contratante, com: descrição de atividades a serem desenvolvidas, relatórios e diagramas com dados relevantes para efeito decisório, responsáveis pelas atividades, cronograma de implementação, compondo o documento denominado "Projeto Executivo" tendo a visibilidade completa do projeto e seus status evolutivo. O documento deve ser entregue para contratante, analisado e aceito pelo responsável técnico da contratante;

3.8.13 A contratada deverá apresentar em reunião a conclusão do projeto com a entrega do documento "Projeto Executivo" completo, contendo todas as informações da operação, arquivos de backup das configurações e visão estratégia;

3.8.14 É responsabilidade da contratada falhas ou erros de instalação provenientes das operações de instalação e configuração;

3.8.15 Os profissionais alocados para a instalação por parte da contratada deverão ter conhecimento pleno nas melhores práticas de configuração do produto e fabricantes;

3.8.16 As senhas configuradas pela contratada no ambiente durante a instalação deverão ter requisito mínimo de 08 (outo) caracteres contendo letras maiúsculas, minúsculas e caracteres especiais;

3.8.17 Os profissionais técnicos alocados na operação pela contratada deverá estar devidamente identificado com uniforme bem como crachá de identificação;

3.8.18 A contratante deverá designar um profissional para acompanhar o processo de implementação, com a finalidade de esclarecimentos sobre o ambiente;

4. <u>ITEM 04: Serviços Gerenciados de Backup</u>

4.1. <u>Ferramenta de backup em nuvem e Data Center</u>

4.1.1. Será de responsabilidade da contratada implementar e configurar o software de transferência de backup local para o repositório na nuvem, de acordo com as políticas atuais da FEMA.

4.1.2. A ferramenta deve estar hospedada em Data Center com

certificação Tier III ou ISO27001 ou SOC 2 Type 2;

4.1.3. A contratada deverá ofertar o armazenar o backup da contratante em nuvem, com backups diários, com no mínimo as seguintes características:

4.1.4. Deverá conter um espaço mínimo liquido de 2TB de armazenamento em nuvem;

4.1.5. A solução deverá conter compactação e/ou aceleração WAN, para menor carga de utilização dos links de internet da contratante;

4.1.6. O licenciamento e operação do ambiente em nuvem é de total responsabilidade da contratada;

4.1.7. O armazenamento de dados da contratante deverá estar localizado no estado de São Paulo, mantendo assim uma menor latência na comunicação e transferência de dados;

4.1.8. A contratada deverá garantir a segurança da informação dos dados e estrutura em nuvem que irá hospedar os dados de backup da contratante. Se responsabilizando por qualquer dano causado a eles;

4.1.9. Os backups deverão estar criptografados com um mínimo de 256 bits;

4.1.9.1. Estar localizado no Brasil, ponto de maior concentração da estrutura do CONTRATANTE; estrutura física dedicada ao serviço de hospedagem, de modo a garantir um ambiente seguro e controlado e possuir ambientes definidos para computadores, sistemas de armazenamento, rede, administração predial, NOC, SOC e sala para clientes;

4.1.9.2. O data center deverá possuir a certificação Tier III ou ISO27001 ou SOC 2 Type 2;

4.1.10. Instalações Físicas

4.1.10.1. Deverá possuir vias de energia elétrica e lógica em alta disponibilidade;

4.1.10.2. Possuir rack do tipo gabinete de 19";

4.1.10.3. Sistema de proteção contra descargas eletromagnéticas, descargas atmosféricas e aterramento;

4.1.11. Energia Elétrica

4.1.11.1. Alimentação elétrica redundante;

4.1.11.2. Total independência no fornecimento de energia na eventualidade de falha na subestação que atende ao data center;

4.1.11.3. Solução de grupo gerador redundante e independente (n+1), com acionamento automático na eventualidade de interrupção no fornecimento de energia e com capacidade mínima de funcionamento por 72 horas com combustível local;

4.1.12. Climatização

4.1.12.1. Sistema de climatização redundante (n+1), refrigerado por formas diferentes;

4.1.13. Proteção Contra Incêndio

4.1.13.1. Dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça);

4.1.13.2. Sistema automático de extinção de incêndios, baseado em agentes gasosos não poluentes, com ação baseada na quebra das moléculas de Oxigênio, do tipo FM200 e/ou FE227, ou equivalente, não nocivos aos equipamentos e seres humanos e que atenda a padrões internacionais;

4.1.14. Segurança Física

4.1.14.1. Disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos;

4.1.14.2. Mecanismos efetivos de controle de entrada e saída de pessoas que acessem e façam uso do IDC, bem como de registros passíveis de posterior pesquisa;

4.1.14.3. Câmeras de circuito interno de televisão, monitoradas e gerenciadas, cujas imagens possam ser posteriormente consultadas e viabilizem o rastreamento de pessoas dentro do IDC;

4.1.14.4. Acesso ao local através de leitura biométrica;

4.1.14.5. O Datacenter deverá possuir vigilância patrimonial 24 horas por dia, 7 dias por semana, 365 dias por ano, permitindo apenas a entrada de pessoas autorizadas e devidamente identificadas;

4.1.15. Estrutura de Telecomunicações

4.1.15.1. Utilizar protocolo de roteamento inteligente para garantir um gerenciamento dinâmico e otimizado dos múltiplos links, assegurar um melhor desempenho no acesso e maior redundância com relação à disponibilidade do acesso;

4.1.15.2. Possuir conexões redundantes responsáveis pelo tráfego interno, facilitando monitoramento e administração em diferentes pontos do data center;

4.1.15.3. Preferencialmente, possuir Pontos de Troca de Tráfego e Acordos de Peering que possam otimizar custos e benefícios com possíveis parceiros do CONTRATANTE;

4.2. Deverá ser construída uma rede local logicamente isolada para a CONTRATANTE dentro do Datacenter. Esta construção deverá ser feita através de VLANs configuradas sobre switches redundantes, permitindo a construção de múltiplos segmentos lógicos de rede para acomodar as tecnologias necessárias para aplicativos, backup de dados, monitoramento, gestão remota de aplicações, dentre outras.

4.3. Gestão de backup nuvem

4.3.1. A contratada deverá administrar e monitorar o sistema de backup descrito nesse documento;

4.3.2. Será de responsabilidade da contratada manter o pleno funcionamento da política de cópia de backup, de acordo com a rotina de backup estabelecida pela contratante;

4.3.3. Deverá monitorar diariamente, os relatórios de cópia de backup gerados ao concluir a tarefa, caso apresente algum erro ou anomalia na execução na tarefa, será de responsabilidade da contratada efetuar correção ou ajuste técnico para a normalização do mesmo, garantindo o pleno funcionamento da solução;

4.3.4. A contratada deverá fornecer mensalmente, toda primeira segunda-feira do mês deverá ser entregue a contratante, um relatório com o resumo de execução de cada tarefa de cópia de backup, durante ao mês anterior, documento denominado "Relatório de Backup Nuvem Diário – MÊS_ANO", a nomenclatura deverá variar de acordo com mês e ano corrente;

4.3.5. Deverá ser de responsabilidade da contratada garantir integridade da cópia do backup LOCAL para NUVEM;

4.3.6. A contratada deverá fornecer mensalmente, um relatório com o resumo da execução dos testes automáticos de integridade das cópias de backups, referente ao mês anterior, documento denominado "Relatório de Teste de Cópia de Backup - MÊS_ANO", a nomenclatura deverá variar de acordo com mês e ano corrente;

4.3.7. A contratada deverá ser responsável por executar as restaurações conforme a manda da contratante;

4.3.8. Para controle, deverá ser entregue a contratante, um relatório de todas restaurações executadas, com data, motivo, objeto e solicitante, referente ao mês anterior, documento denominado "Relatório de Restauração de Backup em Nuvem - MÊS_ANO", a nomenclatura deverá variar de acordo com mês e ano corrente;

4.3.9. Deverá ser realizada de maneira mensal uma reunião presencial com o gestor do contrato, onde a contratada deverá apresentar o relatório mensal;

C.L. FEMA
FLS. nº 184

ANEXO II
MODELO SUGERIDO DE PROPOSTA COMERCIAL
(Em papel timbrado da licitante)
PROCESSO LICITATÓRIO N.º 012/2020
CONVITE N.º 004/2020

1 – IDENTIFICAÇÃO DA EMPRESA

RAZÃO SOCIAL:		
CNPJ/MF:	INSCRIÇÃO ESTADUAL OU MUNICIPAL:	
ENDEREÇO:		N.º:
BAIRRO:	CIDADE:	
CEP:	ESTADO:	
FONE:	ENDEREÇO ELETRÔNICO:	

2 – OBJETO

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

3 - PREÇOS

Os preços ofertados são os seguintes:

LOTE - SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO				
ITEM	**DESCRIÇÃO**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Serviços Gerenciados de Segurança da Informação	1		
2	Serviço de Proteção para Estações de Trabalho	1		
3	Serviço de Suporte Técnico e Monitoramento de Infraestrutura	1		
4	Serviço de Backup em Nuvem	1		

Declaramos total concordância com as condições estabelecidas no edital da presente licitação.

Declaramos, também, que nos valores acima ofertados estão incluídas todas as despesas necessárias ao cumprimento do objeto contratual, observando-se que é obrigação da contratada garantir as alterações legais, corretivas e evolutivas dos softwares, durante toda a vigência contratual.

Declaramos ainda, que os serviços prestados serão realizados de acordo com as especificações do Anexo I – Memorial descritivo.

VALIDADE DA PROPOSTA

C.L. FEMA
FLS. nº 185

A validade da Proposta é de: _____ dias (mínimo de 60 dias)

Dados bancários para pagamento:

Banco: _____

Agência: _____ Conta corrente n.º _____ Dígito n.º_____

Dados do responsável pela assinatura do contrato:

Nome: ----------

Cargo: ----------

CPF: ---------- - RG: ---------- - ORGÃO EMISSOR

Data de Nascimento: XX/XX/XXXXX

Endereço residencial completo: ----------

E-mail institucional ----------

E-mail pessoal: ----------

Telefone(s): (XX) XXXXXXXXXXXXXXXX

[LOCAL], [DIA] de [MÊS] de 2020.

Razão Social da Empresa
Nome do responsável/procurador
Cargo do responsável/procurador
N.º do documento de identidade

C.L. FEMA
FLS. nº 186

ANEXO III
[Em papel timbrado da licitante]
(MODELO)

DECLARAÇÃO DE PLENO ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO

PROCESSO LICITATÓRIO Nº 012/2020
CONVITE Nº 004/2020

À FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS
At. - Pregoeira Oficial

[RAZÃO SOCIAL], estabelecida na [ENDEREÇO COMPLETO], inscrita no CNPJ sob nº [CNPJ], neste ato representada pelo seu [REPRESENTANTE/SÓCIO/PROCURADOR], no uso de suas atribuições legais, vem DECLARAR para efeito do cumprimento ao estabelecido no inciso VII do artigo 4º da Lei Federal n.º 10.520 de 17.07.2002, sob as penalidades cabíveis, que cumpre plenamente as exigências e os requisitos de habilitação previstos no instrumento convocatório do CONVITE referenciado, realizado pela FEMA.

Por ser verdade assina o presente.

[LOCAL], [DIA] de [MÊS] de 2020.

Razão Social da Empresa
Nome do responsável/procurador
Cargo do responsável/procurador
N.º do documento de identidade

C.L. FEMA
FLS. nº 187

ANEXO IV

[Em papel timbrado da licitante]

(MODELO)

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO

PROCESSO LICITATÓRIO Nº 012/2020
CONVITE Nº 004/2020

À FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS
At. - Pregoeira Oficial

[RAZÃO SOCIAL], estabelecida na [ENDEREÇO COMPLETO], inscrita no CNPJ sob n.º [CNPJ], neste ato representado pelo seu [REPRESENTANTE/SÓCIO/PROCURADOR], no uso de suas atribuições legais, vem **DECLARAR**, para fins de participação no processo licitatório em pauta, sob as penas da Lei, que inexiste qualquer fato impeditivo à sua participação na licitação, que não está declarada inidônea para licitar ou contratar com a Administração Pública, nos termos do artigo 87, IV, c/c o artigo 6º, XI da Lei n.º 8.666/93; que não está suspensa temporariamente de participação em licitação e impedida de contratar com a FEMA, nos termos do artigo 87, III, c/c o artigo 6º, XII da Lei nº 8.666/93; que não está impedida de licitar e contratar com a Administração direta e indireta da Prefeitura Municipal de Assis, nos termos do artigo 7º da Lei Federal nº 10.520/02; e, que se compromete a comunicar ocorrência de fatos supervenientes.

Por ser verdade assina o presente.

[LOCAL], [DIA] de [MÊS] de 2020.

Razão Social da Empresa
Nome do responsável/procurador
Cargo do responsável/procurador
N.º do documento de identidade

C.L. FEMA
FLS. nº 188

ANEXO V
[Em papel timbrado da licitante]
(MODELO)

DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

PROCESSO LICITATÓRIO Nº 012/2020
CONVITE Nº 004/2020

À FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS
At. - Pregoeira Oficial

[RAZÃO SOCIAL], com sede na [ENDEREÇO COMPLETO], inscrita no CNPJ sob o nº. [CNPJ], DECLARA, para fins do disposto na Lei Complementar nº 123/2006 e alterações posteriores, sob as sanções administrativas cabíveis e sob as penas da lei, que esta Empresa, na presente data, enquadra-se como:
[ ] **MICROEMPRESA**, conforme inciso I do artigo 3º da Lei Complementar nº 123, de 14/12/2006.

[ ] **EMPRESA DE PEQUENO PORTE**, conforme inciso II do artigo 3º da Lei Complementar nº 123, de 14/12/2006.
Declara, ainda, que a empresa não possui qualquer dos impedimentos previstos nos §§ 4º e seguintes todos do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006, alterada pela Lei Complementar nº 147, de 7 de agosto de 2.014.

Por ser verdade assina o presente.

[LOCAL], [DIA] de [MÊS] de 2020.

Razão Social da Empresa
Nome do responsável/procurador
Cargo do responsável/procurador
N.º do documento de identidade

Fundação Educacional do Município de Assis
Campus "José Santilli Sobrinho"

ANEXO VI
[Em papel timbrado da licitante]
(MODELO)
DECLARAÇÃO DE REGULARIDADE INCISO XXXIII, ARTIGO 7° DA CRFB/88.

PROCESSO LICITATÓRIO Nº 012/2020
CONVITE Nº 004/2020

À FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS
At. - Pregoeira Oficial

Eu, [NOME], representante legal da empresa [RAZÃO SOCIAL], interessada em participar do CONVITE Nº XXX/2020, da FEMA, DECLARO, sob as penas da lei que, nos termos do inciso V do artigo 27 da Lei nº 8.666, de 21 de junho de 1.993 e alterações, a empresa encontra-se em situação regular perante o órgão ministerial competente, no que se refere à observância do disposto no inciso XXXIII do artigo 7º da Constituição Federal, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva:

[ ] Emprega menor, a partir de quatorze anos, na condição de aprendiz.
(Observação: em caso afirmativo, assinalar a ressalva acima)

Por ser verdade assina a presente.

[LOCAL], [DIA] de [MÊS] de 2020.

Razão Social da Empresa
Nome do responsável/procurador
Cargo do responsável/procurador
N.º do documento de identidade

Fundação Educacional do Município de Assis
Campus "José Santilli Sobrinho"

ANEXO VII

PROCESSO LICITATÓRIO Nº 012/2020
CONVITE Nº 004/2020

DECLARAÇÃO RECEBIMENTO DE EDITAL

Declaramos que, na data de _____/_____/2020, recebemos da Fundação Educacional do Município de Assis – FEMA, cópia do edital de licitação na modalidade Convite e seus anexos, referente à CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, deverão ser entregues lacrados, à Comissão Permanente de Licitação, ***às 09h30min do dia 27 de fevereiro de 2020***, no Setor de Compras e Licitações, sito a Av. Getúlio Vargas, 1.200 – Vila Nova Santana Assis.

Assis, _____de _____ de 2020.

Nome do recebedor: _____
Cargo do responsável/procurador:_____
N.º do documento de identidade:_____

CARIMBO DA EMPRESA:

Fundação Educacional do Município de Assis
Campus "José Santilli Sobrinho"

ANEXO VIII
(MODELO)

DECLARAÇÃO DE INTERESSE EM PARTICIPAÇÃO NA LICITAÇÃO

CONVITE N.º 004/2020
DATA INÍCIO: 14/02/2020
DATA ENCERRAMENTO: 27/02/2020 ÀS 09H30MIN.

À Fundação Educacional do Município de Assis - FEMA

A empresa (razão social) _____, CNPJ nº _____, estabelecida na ____ (endereço completo), telefone ( )_____-_____, e-mail _____, ***DECLARA*** interesse na participação do Convite nº 004/2020, cujo objeto é a CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

(cidade),_____de _____ de 2020.

Nome e Assinatura do representante legal
CPF n.º _____
RG n.º _____

Carimbo da empresa:

Fundação Educacional do Município de Assis
Campus "José Santilli Sobrinho"

ANEXO IX
MINUTA DO TERMO DE CONTRATO
PROCESSO LICITATÓRIO N.º 012/2020
CONVITE N.º 004/2020

Pelo presente instrumento particular de contrato, de um lado a FEMA – FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS - FEMA, com sede na Avenida Getúlio Vargas nº 1200, Vila Nova Santana, Assis/SP, inscrito no CNPJ sob o nº 51.501.559/0001-36, neste ato representada pelo seu Diretor Executivo, Eduardo Augusto Vella Gonçalves, portador do portador do RG nº 23.348.242-8 - SSP/SP e CPF/MF nº 204.560.678-33, morador na cidade Assis, Estado de São Paulo, na Rua Van Gogh, n.º 50 - Residencial Renascence, doravante denominada CONTRATANTE e, de outro lado, a empresa ----------, inscrita no CNPJ sob o nº. ----------, inscrição estadual ou municipal nº ---------, com sede na [endereço completo], [Bairro], [CEP], [Município] – [Estado], daqui por diante denominada **CONTRATADA** neste ato legalmente representada pelo Sr. **[nome do representante (s)]**, portador da cédula de identidade RG nº ----------, expedido pelo ------/--- e inscrito no CPF sob o nº ----------, morador na [endereço completo], [Bairro], [CEP], [Município] – [Estado], as partes assim identificadas pactuam o presente contrato, que reger-se-á segundo disposições da Lei n.º 10.520/02, Lei 8.666/93 e suas alterações, tanto pelas cláusulas e condições do CONVITE n.º 004/2020, com todos os seus anexos, que fazem parte integrante deste, bem como às seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente instrumento tem por objeto a CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

1.2. O fornecimento do objeto deste Contrato obedecerá ao estipulado neste instrumento, bem como às disposições constantes dos documentos adiante enumerados, que, independentemente de transcrição, fazem parte integrante e complementar deste contrato:

1.2.1. Proposta da **CONTRATADA**;

1.2.2. Edital do CONVITE Nº 004/2020 e seus anexos;

1.2.3. Termo de Referência.

1.3. Os documentos referidos na presente Cláusula são considerados suficientes para, em complemento a este Contrato, definir a sua intenção e, desta forma, reger sua execução dentro do mais alto padrão da técnica

atual.

CLÁUSULA SEGUNDA - DOS PREÇOS

2.1. Importa o presente contrato no valor global de R$ XXXXXXXXX (XXXXXXXXXX), proveniente do valor mensal de R$ XXXXXXXXXX (XXXXXXXXXX) pelo período de 12 (doze) meses, decorrente do valor constante da proposta vencedora do processo licitatório n.º XXXX/2020.

2.2. Nos preços acima estipulados estão inclusas todas as despesas sobre o objeto contratado tais como: tributos, fretes, seguros, encargos sociais e demais encargos indispensáveis ao perfeito cumprimento das obrigações decorrentes deste instrumento.

CLÁUSULA TERCEIRA - DAS CONDIÇÕES DE PAGAMENTO

3.1. O início da cobrança dos serviços será na data da efetiva disponibilização do mesmo, para uso da CONTRATANTE, conforme solicitação e cronograma de implantação.

3.2. O pagamento referente ao mês de ativação ou de desativação dos serviços será proporcional ao número de dias do mês comercial, considerado este como sendo de 30 (trinta) dias corridos.

3.3. A FEMA efetuará pagamento mensalmente através do sistema bancário;

3.3.1. O pagamento será efetuado em até 5 (cinco) dias útil contados da apresentação da fatura/nota fiscal à CONTRATANTE;

3.3.2. Caso o vencimento do prazo de pagamento da Nota Fiscal ocorra fora do calendário semanal ou de expediente bancário, o pagamento será efetuado na próxima data do calendário, imediatamente posterior ao vencimento, não incidindo qualquer compensação financeira neste período;

3.4. Não será admitida proposta com condição de pagamento antecipado ou de prazo contado da data de emissão da nota fiscal.

3.5. Nenhum pagamento será efetuado ao licitante vencedor enquanto pendente de liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

3.6. Os valores ofertados pela CONTRATADA em sua proposta comercial já consideraram todos os encargos incidentes sobre o objeto deste Contrato, não sendo aceita reivindicação posterior para sua inclusão nesses valores, salvo se houver comprovação de que são novos e criados por ato de governo.

3.7. A CONTRATANTE se reserva o direito de suspender o pagamento se o serviço for prestado em desacordo com as especificações constantes deste Contrato, ou se houver qualquer erro ou irregularidade em relação a dados constantes da fatura/nota fiscal apresentada, o que não acarretará para a CONTRATANTE a responsabilidade por quaisquer ônus decorrentes desse não

pagamento, como multas e correções.

3.8. Os pagamentos serão efetuados observando-se a ordem cronológica estabelecida no art. 5º da Lei n.º 8.666/93.

3.9. O pagamento somente será efetuado se a CONTRATANTE atestar a execução satisfatória do serviço.

3.10. O pagamento efetuado não implica reconhecimento pela CONTRATANTE de adimplemento por parte da CONTRATADA relativamente às obrigações previdenciárias, sociais, trabalhistas, tributárias e fiscais, nem novação em relação a qualquer regra constante destas especificações.

CLÁUSULA QUARTA – DA VIGÊNCIA

4.1. A vigência do presente contrato será de 12 (doze) meses, contados a partir da assinatura do presente termo, podendo vir a sofrer prorrogações, desde que justificado, conforme acordo entre as partes, através de respectivo termo, antes do seu vencimento, com adequação aos termos do inciso IV do artigo 57 da 8.666/93.

CLÁUSULA QUINTA – DAS ALTERAÇÕES CONTRATUAIS

5.1. Este Contrato poderá ser alterado, mediante Termo Aditivo e com as devidas justificativas, nos casos previstos no art. 65, da Lei nº 8.666/93.

CLÁUSULA SEXTA – DO REAJUSTE

6.1. Os valores indicados pela CONTRATADA em sua proposta comercial não serão reajustados durante o período de 12 (doze) meses, na forma da legislação vigente.

6.2. Poderão ser alterados após esse período mediante Índice Geral de Preços do Mercado (IGP-M) acumulado em 12 (doze meses).

6.4. Respeitado o valor mínimo pactuado pelo período de vigência do Contrato, fica reservado à "Contratante" o direito à negociação dos índices de reajuste.

6.5. Eventual alteração de valores em decorrência de reequilíbrio econômico-financeiro do Contrato só será examinada mediante apresentação de documentos que comprovem, de forma inequívoca, a alteração da relação encargos/retribuição inicialmente pactuada.

CLÁUSULA SÉTIMA – DA FISCALIZAÇÃO

7.1. A fiscalização dos serviços será efetuada pelo Centro de Pesquisa em Informática - CEPEIN.

7.2. Deverão ser assegurados à CONTRATANTE amplos poderes para fiscalizar e acompanhar o serviço contratado, bem como o direito de obter os esclarecimentos que julgar necessários, devendo a CONTRATADA fornecer relatórios ou quaisquer informações que lhe forem solicitados.

7.3.- A ação fiscalizadora da CONTRATANTE não fará cessar nem diminuir a responsabilidade da CONTRATADA pelo perfeito cumprimento das

obrigações estipuladas no instrumento convocatório, e, neste Contrato ou por irregularidades constatadas, nem por quaisquer danos causados, inclusive a terceiros.

CLÁUSULA OITAVA – DOS RECURSOS FINANCEIROS

8.1. As despesas decorrentes da execução deste contrato correrão por conta das dotações próprias do orçamento vigente até o encerramento do atual ano civil, classificadas e codificadas sob os números: _____

_____

_____

_____

CLÁUSULA NONA - DAS RESPONSABILIDADES DA CONTRATADA

9.1. Além das obrigações resultantes da Lei Federal n.º 8.666/1993, e, as constantes no edital e seus anexos, a CONTRATADA se obriga a:

9.1.1. assumir responsabilidade civil relativamente a qualquer dano que o serviço por ela prestado venha a causar ao patrimônio público, ao pessoal da CONTRATANTE ou a terceiros.

9.1.2. responsabilizar-se pelos encargos trabalhistas, sociais previdenciários, fiscais e securitários resultantes da execução deste Contrato, devendo remeter à CONTRATANTE os respectivos comprovantes, sempre que exigidos.

9.1.3. Em caso de a CONTRATANTE ser judicialmente condenada ao pagamento de quaisquer ônus referidos no subitem acima, a CONTRATADA deverá ressarci-la dos valores correspondentes, acrescidos de 20% (vinte por cento) a título de honorários.

9.1.4. A CONTRATADA deverá manter, ao longo da execução deste Contrato, a qualidade do serviço previsto no TERMO DE REFERÊNCIA, sendo obrigada a refazer, a qualquer tempo, serviço prestado que apresente qualquer tipo de defeito.

9.1.5. A CONTRATADA será obrigada a manter, durante a vigência do Contrato, as condições de habilitação exigidas no processo licitatório.

CLÁUSULA DÉCIMA – DA RESPONSABILIDADE DE CONTRATANTE

10.1. Fornecer à **CONTRATADA**, todas as informações relacionadas com o objeto do presente contrato;

10.2. Pagar à **CONTRATADA** na forma estabelecida neste instrumento, efetuando a retenção dos tributos devidos, consoante a legislação vigente;

10.3. Acompanhar e fiscalizar, através de servidor designado pela Administração, o cumprimento deste instrumento, anotando em registro próprio as falhas detectadas e comunicando as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas;

10.4. Exigir a apresentação de notas fiscais com as requisições fornecidas, recibos, atestados, declarações e outros documentos que comprovem as

operações realizadas, o cumprimento de pedidos, o atendimento de providências, o compromisso de qualidade, etc.

CLÁUSULA DÉCIMA PRIMEIRA – DA RESCISÃO

11.1. O contrato poderá ser rescindido de pleno direito, quando:

11.1.1. A inexecução total ou parcial do CONTRATO enseja a sua rescisão pela CONTRATANTE, com as consequências previstas nos artigos 77 e 80 da Lei Federal nº 8.666/93, sem prejuízo da aplicação das penalidades a que alude o artigo 87 da mesma Lei;

11.1.2. Constituem motivos para rescisão os previstos no artigo 78 da Lei Federal nº 8666/93 e alterações posteriores.

11.1.3. Nos termos do art. 79 da Lei Federal nº 8.666/93, a rescisão contratual poderá ser:

a) Determinada por ato unilateral e escrito da CONTRATANTE, nos casos enumerados nos incisos I, XII e XVII do artigo 78 da Lei nº 8.663/93;

b) Amigável, por acordo entre as partes, mediante autorização escrita e fundamentada da CONTRATADA, reduzida a termo, desde que haja conveniência da CONTRATANTE;

c) Judicial, nos termos da legislação;

11.1.4. Quando a rescisão ocorrer com base nos incisos XII a XVII do artigo 78 da Lei Federal nº 8.666/93, sem que haja culpa da CONTRATADA, será esta ressarcida dos prejuízos regularmente comprovados que houver sofrido, tendo ainda direito aos pagamentos devidos pela execução do CONTRATO até a data da rescisão.

CLÁUSULA DÉCIMA SEGUNDA – SANÇÕES ADMINISTRATIVAS

12.1. A recusa injustificada da adjudicatária em aceitar ou retirar o termo de contrato equivalente, dentro do prazo estabelecido caracteriza o descumprimento total da obrigação assumida, sujeitando-o a juízo da Administração, nos termos da legislação municipal:

a) À multa de 30% (trinta por cento) sobre o valor do contrato;

b) Ao pagamento correspondente à diferença de preço decorrente de nova licitação ou contratação, para o mesmo fim;

12.2. Pela inexecução total do contrato, será aplicada à Contratada a multa de 30% (trinta por cento) sobre o valor total do ajuste;

12.3. Pela inexecução parcial do contrato, será aplicada à Contratada a multa de 20% (vinte por cento) sobre o valor da obrigação não cumprida.

12.4. Pelo atraso injustificado a CONTRATADA incorrerá em multa diária de 0,1% (um décimo por cento) sobre o valor do contrato, excluída, quando for o caso, a parcela correspondente aos impostos incidentes, quando destacados no documento fiscal, sendo que a aplicação da multa terá inicio no primeiro dia seguinte ao término do prazo contratual ou de execução do serviço.

C.L. FEMA
FLS. nº 197

12.5. As multas a que aludem os subitens anteriores não impedem que a Administração rescinda unilateralmente o contrato e aplique outras sanções previstas nas Leis Federais e Municipais citadas no preâmbulo deste, a saber:
12.5.1. Advertência, por escrito, no caso de pequenas irregularidades.
12.5.1.1. A sanção de advertência poderá ser aplicada nos seguintes casos:
I. Descumprimento das determinações necessárias à regularização das faltas ou defeitos observados na prestação dos serviços;
II. Outras ocorrências que possam acarretar transtornos no desenvolvimento dos serviços da FEMA, desde que não caiba a aplicação de sanção mais grave.
12.5.2. Suspensão temporária do direito de licitar e impedimento de contratar com a Administração, pelo prazo de até dois anos, quando da inexecução contratual sobrevier prejuízo para a Administração;
12.5.2.1. A penalidade de suspensão será cabível quando o licitante participar do certame e for verificada a existência de fatos que o impeçam de contratar com a Administração Pública. Caberá ainda a suspensão quando a licitante, por descumprimento de cláusula contratual tenha causado transtornos no desenvolvimento dos serviços da FEMA.
12.5.3. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação.
12.5.3.1. Se o licitante deixar de entregar a documentação ou apresentá-la falsamente, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará, pelo prazo de até 5 (cinco) anos, impedido de contratar com a Administração Pública, sem prejuízo das multas previstas no edital e das demais cominações legais.
12.5.4. Verificado que a obrigação foi cumprida com atraso injustificado caracterizando a inexecução parcial, a FEMA poderá reter preventivamente, o valor da multa dos eventuais créditos que a Contratada tenha direito, até a decisão definitiva, assegurada a ampla defesa.
12.5.4.1. Caso a Contratada tenha prestado garantia, e esta for insuficiente para cobrir o valor da multa, será retida a diferença, nos termos do subitem 12.5.4.
12.5.4.2. Se a FEMA decidir pela não aplicação da multa, o valor retido será devolvido à Contratada.
12.6. Independentemente das sanções retro a CONTRATADA ficará sujeita, ainda, à composição das perdas e danos causados à Administração e decorrentes de sua inadimplência, bem como arcará com a correspondente diferença de preços verificada em nova contratação, na hipótese de os demais classificados não aceitarem a contratação pelos

C.L. FEMA
FLS. nº 198

mesmos preços e prazos fixados pelo inadimplente.

12.7. São assegurados nos termos legais os prazos para exercício do direito da ampla defesa e do contraditório, na aplicação das sanções.

CLÁUSULA DÉCIMA TERCEIRA – DO SUPORTE LEGAL

13.1. A execução do presente contrato e aos casos omissos aplicam-se as disposições contidas na Lei nº. 8.666/93, de 21 de junho de 1993, e suas alterações.

CLÁUSULA DÉCIMA QUARTA – DAS CONDIÇÕES DE HABILITAÇÃO

14.1. A CONTRATADA deverá observar para que durante toda a vigência do contrato, seja mantida a compatibilidade com as obrigações assumidas, as condições de habilitação e qualificação exigidas para a contratação, conforme a Lei nº. 8.666/93 e alterações.

CLÁUSULA DÉCIMA QUINTA - DO FORO

15.1. Fica eleito o foro da Comarca de Assis/SP, com exclusão de outro qualquer, para dirimir as questões oriundas do presente contrato que não forem resolvidas por via administrativa na forma de Código Civil.

E, por estarem justas e contratadas, assinam as partes o presente instrumento em 03 (três) vias de igual teor e forma na presença de 02 (duas) testemunhas adiante indicadas.

Assis, XX de XXXX de 2020.

AS PARTES:

1) FEMA – FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS
CONTRATANTE

Eduardo Augusto Vella Gonçalves
Diretor Executivo

2) NOME LICITANTE VENCEDOR

NOME REPRESENTANTE LEGAL
CARGO

Testemunhas:

NOME
RG N.º

NOME
RG N.º

Fundação Educacional do Município de Assis
Campus "José Santilli Sobrinho"

"EXTRATO DE TERMO CONTRATO Nº XXX/2020"

Ref.: Processo n.º 012/2020 – CONVITE n.º 004/2020 - Contratante: FEMA – Fundação Educacional do Municio de Assis - Contratada: ---------- – CNPJ/MF n. ---------- - Objeto: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO em conformidade com as especificações no Anexo I - Termo de Referência. - Valor Mensal: R$ ----- - Valor Anual: R$ ---------- - Prazo de vigência: 12 (doze) meses - Pagamento: Mensal.

Assis, XX de XXXXXXXX de 2020.

Eduardo Augusto Vella Gonçalves
Diretor Executivo

Fundação Educacional do Município de Assis
Campus "José Santilli Sobrinho"

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO
(Contratos)

CONTRATANTE: FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS
CONTRATADO: ----------
CONTRATO Nº (DE ORIGEM): -------/2020
OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO COMO SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.
ADVOGADO: ----------.

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:
a) o ajuste acima referido estará sujeito à análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;
b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, conforme dados abaixo indicados, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;
c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;
d) Qualquer alteração de endereço – residencial ou eletrônico – ou telefones de contato deverá ser comunicada pelo interessado, peticionando no processo.

2. Damo-nos por NOTIFICADOS para:
a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;
b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

Assis, XX de XXXX de 2020.

Fundação Educacional do Município de Assis
Campus "José Santilli Sobrinho"

GESTOR DO ÓRGÃO/ENTIDADE:
Nome: ----------
Cargo: ----------
CPF: ---------- - RG: ---------- - ORGÃO EMISSOR
Data de Nascimento: XX/XX/XXXXX
Endereço residencial completo: ----------
E-mail institucional ----------
E-mail pessoal: ----------
Telefone(s): (XX) XXXXXXXXXXXXXXXX

Assinatura: _____

Responsáveis que assinaram o ajuste:
Pelo **CONTRATANTE**:
Nome: ----------
Cargo: ----------
CPF: ---------- - RG: ---------- - ORGÃO EMISSOR
Data de Nascimento: XX/XX/XXXXX
Endereço residencial completo: ----------
E-mail institucional ----------
E-mail pessoal: ----------
Telefone(s): (XX) XXXXXXXXXXXXXXXX

Assinatura: _____

Pela **CONTRATADA:**
Nome: ----------
Cargo: ----------
CPF: ---------- - RG: ---------- - ORGÃO EMISSOR
Data de Nascimento: XX/XX/XXXXX
Endereço residencial completo: ----------
E-mail institucional ----------
E-mail pessoal: ----------
Telefone(s): (XX) XXXXXXXXXXXXXXXX

ASSINATURA:_____