PREGÃO ELETRÔNICO Nº 20190012 - ETICE/DITEC

PROCESSO Nº 09551772/2019

UASG: 943001

Número Comprasnet: 15962019

A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ - ETICE, por intermédio do pregoeiro e do membro da equipe de apoio designados por ato do Governador do Estado, que ora integra os autos, torna público que realizará licitação na modalidade PREGÃO, para REGISTRO DE PREÇO, na forma ELETRÔNICA.

1. DO TIPO: Menor Preço.

2. DO REGIME DE EXECUÇÃO INDIRETA: Empreitada por preço unitário.

3. DA BASE LEGAL: Lei Federal nº 10.520, de 17 de julho 2002, Lei Complementar Federal nº 123, de 14 de dezembro de 2006, Lei Complementar Estadual nº 65, de 3 de janeiro de 2008, Lei Complementar Estadual nº 134, de 7 de abril de 2014, Decretos Estaduais nº 27.624, de 22 de novembro 2004, nº 33.326, de 29 de outubro de 2019, nº 32.718, de 15 de junho de 2018, nº 32.824 de 11 de outubro de 2018, Regulamento de Licitações e Contratações da ETICE e subsidiariamente a Lei Federal nº 13.303, de 30 de junho de 2016, e o disposto no presente edital e seus anexos.

4. OBJETO: Registro de preços para futuras e eventuais **serviços de fornecimento, aquisição, manutenção de Solução Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Empresa de Tecnologia da Informação do Ceará**, de acordo com as especificações e quantitativos previstos no Anexo I - Termo de Referência deste edital.

5. DO ACESSO AO EDITAL E DO LOCAL DE REALIZAÇÃO E DO PREGOEIRO

5.1. O edital está disponível gratuitamente nos sítios www.portalcompras.ce.gov.br e www.comprasnet.gov.br.

5.2. O certame será realizado por meio do sistema Comprasnet, no endereço eletrônico www.comprasnet.gov.br, pelo pregoeiro Raimundo Vieira **Coutinho**, telefone: (85) 3459-6563.

6. DAS DATAS E HORÁRIOS DO CERTAME

6.1. INÍCIO DO ACOLHIMENTO DAS PROPOSTAS: 31/01/2020

6.2. DATA DE ABERTURA DAS PROPOSTAS: 12/02/2020, às 08h30min

6.3. INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: 12/02/2020, às 08h30min

6.4. REFERÊNCIA DE TEMPO: Para todas as referências de tempo utilizadas pelo sistema será observado o horário de Brasília - DF.

6.5. Na hipótese de não haver expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data prevista, a sessão será remarcada, para no mínimo 48h (quarenta e oito horas) a contar da respectiva data, exceto quando remarcada automaticamente pelo próprio sistema eletrônico.

7. DO ENDEREÇO E HORÁRIO DA CENTRAL DE LICITAÇÕES

7.1. Central de Licitações - PGE, Av. Dr. José Martins Rodrigues, nº 150, Bairro: Edson Queiroz, Fortaleza - Ceará, CEP: 60.811-520, CNPJ nº 06.622.070.0001-68.

7.2. Horário de expediente da Central de Licitações: das 8h às 12h e de 14h às 18h.

8. DOS RECURSOS ORÇAMENTÁRIOS

8.1. As despesas decorrentes da Ata de Registro de Preços correrão pela fonte de recursos da ETICE, a ser informada quando da lavratura do instrumento de contrato.

9. DA PARTICIPAÇÃO

9.1. Os interessados em participar deste certame deverão estar credenciados junto ao portal de compras do Governo Federal.

9.1.1. As regras para credenciamento estarão disponíveis no sítio constante no subitem 5.2. deste edital.

9.2. Tratando-se de microempresas, empresas de pequeno porte e as cooperativas que se enquadrem nos termos do art. 34, da Lei Federal n° 11.488/2007, e que não se encontram em qualquer das exclusões relacionadas no § 4º do artigo 3º da Lei Complementar nº 123/2006, deverão declarar no Sistema Comprasnet para o exercício do tratamento jurídico simplificado e diferenciado previsto em Lei.

9.3. A participação implica a aceitação integral dos termos deste edital.

9.4. É vedada a participação nos seguintes casos:

9.4.1. Que estejam em estado de insolvência civil, sob processo de falência, dissolução, fusão, cisão, incorporação e liquidação.

9.4.2. Impedidas de licitar e contratar com a Administração.

9.4.3. Suspensas temporariamente de participar de licitação e impedidas de contratar com a Administração.

9.4.4. Declaradas inidôneas pela Administração Pública, enquanto perdurarem os motivos determinantes desta condição.

9.4.5. Servidor público ou empresas cujos dirigentes, gerentes, sócios ou componentes de seu quadro sejam funcionários ou empregados públicos da entidade contratante ou responsável pela licitação.

9.4.6. Estrangeiras não autorizadas a comercializar no país.

9.4.7. Cujo estatuto ou contrato social, não inclua no objetivo social da empresa, atividade compatível com o objeto do certame.

9.4.8. Constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea.

9.4.9. Cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea.

9.4.10. Constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção.

9.4.11. Cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção.

9.4.12. Que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

9.4.13. Empregado ou dirigente da ETICE, como pessoa física.

9.4.14. Quem tenha relação de parentesco, até o terceiro grau civil, com:

9.4.14.1. Dirigente ou empregado da ETICE, neste último caso quando as atribuições do empregado envolvam a atuação na área responsável pela licitação ou contratação.

9.4.14.2. Autoridade do ente público a que a ETICE esteja vinculada.

9.4.15. Cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a ETICE há menos de 6 (seis) meses.

9.4.16. Possuam entre seus dirigentes, gerentes, sócios, responsáveis legais ou técnicos, membros do conselho técnico, fiscal, consultivo, deliberativo ou administrativo, qualquer pessoa que seja membro da Administração da ETICE.

9.4.17. Sob a forma de consórcio, qualquer que seja sua constituição.

9.4.18. As justificativas para a vedação da participação de Consórcios estão a seguir descritas:

9.4.18.1. A vedação de participação de Consórcios de empresas deve levar em consideração que a Jurisprudência do Tribunal de Contas da União, no Acórdão de nº 2303/2015, decidiu que a possibilidade de consórcio é um ato discricionário da Administração Pública, ou seja, é facultado à ETICE a opção de permitir ou não o consórcio nas licitações, conforme os termos do voto: “A jurisprudência consolidada desta Corte considera que a opção em permitir ou não a associação das licitantes em consórcio fica ao alvedrio do administrador”.

9.4.18.2. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida em casos especiais, onde empresas não costumam atender individualmente o objeto litado em razão de sua complexidade, o que não ocorre no caso concreto, tendo em vista que, quando da obtenção das propostas, para composição do mapa de preços, não houve dificuldade; ou seja, o edital não traz em seu Termo de referência nenhuma característica própria que justificasse a admissão de empresas em consórcio.

9.4.18.3. Tendo em vista que é prerrogativa do Poder Público, na condição de Contratante, a escolha da participação, ou não, de empresas constituídas sob a forma de consórcio, conforme se depreende da literalidade da Lei n. 8.666/93, que em seu artigo 33 atribui à Administração a faculdade de admissão de consórcios em licitações por ela promovidas; pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

9.4.18.4. Portanto, a admissão de consórcio no caso concreto atentaria contra o princípio da competitividade, pois permitiria, com o aval do Estado, a união de concorrentes que poderiam muito bem disputar entre si, violando, por via transversa, o princípio da competitividade, atingindo ainda a vantajosidade buscada pela Administração.

9.4.18.5. Ressalte-se que a decisão com relação à vedação à participação de consórcios visa exatamente afastar a restrição à competição, na medida que a reunião de empresas que, individualmente, poderiam prestar os serviços, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluios/carteis para manipular os preços nas licitações.

10. DOS PEDIDOS DE ESCLARECIMENTOS E IMPUGNAÇÕES

10.1. Os pedidos de esclarecimentos e impugnações referentes ao processo licitatório deverão ser enviados ao pregoeiro, até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico, no endereço licitacao@pge.ce.gov.br, até as 17:00, no horário oficial de Brasília/DF. Indicar o nº do pregão e o pregoeiro responsável.

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

10.2. Não serão conhecidas as impugnações apresentadas fora do prazo legal e/ou subscritas por representante não habilitado legalmente.

10.3. As respostas aos pedidos de esclarecimentos e impugnações serão divulgadas no sistema e vincularão os participantes e a administração.

10.4. Acolhida a impugnação contra este edital, será designada nova data para a realização do certame, exceto se a alteração não afetar a formulação das propostas.

11. DA HABILITAÇÃO

11.1. A licitante que for cadastrada no Sistema de Cadastramento Unificado de Fornecedores – SICAF, do Governo Federal ou Certificado de Registro Cadastral (CRC) emitido pela Secretaria do Planejamento e Gestão (SEPLAG), do Estado do Ceará, ficará dispensada da apresentação dos documentos de que tratam os subitens 11.3. e 11.4. deste edital.

11.1.1. A Central de Licitações verificará eletronicamente a situação cadastral, caso esteja com algum(ns) documento(s) vencido(s), a licitante deverá apresentá-lo(s) dentro do prazo de validade, sob pena de inabilitação, salvo aqueles acessíveis para consultas em *sítios* oficiais que poderão ser consultados pelo pregoeiro.

11.1.2. Existindo restrição no cadastro quanto ao documento de registro ou inscrição em entidade profissional competente, este deverá ser apresentado em situação regular, exceto quando não exigido na qualificação técnica.

11.1.3. É dever da licitante atualizar previamente os documentos constantes no SICAF ou CRC para que estejam vigentes na data da abertura da sessão pública.

11.2. Como condição prévia ao exame da documentação de habilitação da licitante detentora da proposta classificada em primeiro lugar, o pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante consulta em sites oficiais.

11.2.1. Constatada a existência de sanção e/ou eventual descumprimento das condições de participação, o pregoeiro reputará a licitante inabilitada.

11.3. A documentação relativa à habilitação jurídica consistirá em:

a) Registro Comercial no caso de empresa individual.

b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedades por ações, documentos de eleição de seus administradores.

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

d) 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.

e) Cédula de identidade, em se tratando de pessoa física.

11.4. A documentação relativa à regularidade fiscal e trabalhista consistirá em:

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ).

b) Certificado de Regularidade do FGTS - CRF, perante o Fundo de Garantia por Tempo de Serviço, atualizado.

c) Prova de regularidade para com as Fazendas: Federal (Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União), Estadual e Municipal do domicílio ou sede da licitante, devidamente atualizada.

d) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e considerando o disposto no art. 3º da Lei nº 12.440, de 7 de julho de 2011.

11.4.1. No caso de pessoa física, esta deverá apresentar o Cadastro de Pessoas Físicas (CPF), ficando dispensada a apresentação dos documentos “a” e “b” do item 11.4. deste edital.

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

11.4.2.1. Havendo restrição quanto à regularidade fiscal e trabalhista da microempresa, da empresa de pequeno porte ou da cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007, será assegurado o prazo de 5 (cinco) dias úteis, contados a partir de declarada a vencedora, para a regularização do(s) documento(s), podendo tal prazo ser prorrogado por igual período, conforme dispõe a Lei Complementar nº 123/2006.

11.4.2.2. A não comprovação da regularidade fiscal e trabalhista, até o final do prazo estabelecido, implicará na decadência do direito, sem prejuízo das sanções cabíveis, sendo facultado ao pregoeiro convocar as licitantes remanescentes, por ordem de classificação.

11.4.3. Para os estados e municípios que emitem prova de regularidade fiscal em separado, as proponentes deverão apresentar as respectivas certidões.

11.5. A documentação relativa à qualificação técnica, consistirá em:

a) Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características com o objeto da licitação, mediante apresentação de atestado(s) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado.

11.6. A documentação relativa à qualificação econômica financeira, consistirá em:

a) Certidão negativa de falência, recuperação judicial ou extrajudicial, expedida pelo distribuidor judicial da sede da pessoa jurídica.

b) Na ausência da certidão negativa, a licitante em recuperação judicial deverá comprovar o acolhimento judicial do plano de recuperação judicial nos termos do art. 58 da Lei nº 11.101/2005. No caso da licitante em recuperação extrajudicial deverá apresentar a homologação judicial do plano de recuperação.

11.6.1. No caso de pessoa física, esta deverá apresentar a Certidão Negativa de Execução Patrimonial expedida em domicílio, ficando dispensada a apresentação dos documentos “a” e “b” do subitem 11.6. deste edital.

11.7. A licitante deverá declarar no sistema Comprasnet, de que não emprega mão de obra que constitua violação ao disposto no inciso XXXIII, do art. 7º, da Constituição Federal**.**

12. DA FORMA DE APRESENTAÇÃO DA PROPOSTA ELETRÔNICA E DOS DOCUMENTOS DE HABILITAÇÃO

12.1. As licitantes encaminharão, até a data e o horário estabelecidos para abertura da sessão pública, exclusivamente por meio do sistema, os documentos de habilitação e a proposta com a descrição do objeto ofertado e o preço, bem como declaração de responsabilidade pela autenticidade dos documentos apresentados, conforme Anexo V - Declaração de autenticidade da documentação deste edital.

12.1.1. A ausência da declaração de autenticidade da documentação não implicará no afastamento imediato da arrematante, por configurar falha formal passível de saneamento nos termos do subitem 22.2 deste edital.

12.2. A proposta deverá explicitar nos campos “VALOR UNITÁRIO (R$)” E “VALOR TOTAL (R$)”, os preços referentes a cada item, incluídos todos os custos diretos e indiretos, em conformidade com as especificações deste edital, inclusive o cálculo da diferença entre o imposto(ICMS) para os itens 9, 10 e 11 do grupo 1, devido à unidade federada de destino e a unidade federada de origem, conforme Emenda Constitucional nº 87/2015. O Campo “descrição detalhada do objeto ofertado” deverá ser preenchido.

12.2.1. A proposta deverá ser anexada, devendo a última folha ser assinada e as demais rubricadas pela licitante ou seu representante legal, redigida em língua portuguesa em linguagem clara e concisa, sem emendas, rasuras ou entrelinhas, com as especificações técnicas, quantitativos, marca/modelo, nos termos do Anexo I - Termo de Referência deste edital.

12.2.2. Prazo de validade não inferior a 90 (noventa) dias, contados a partir da data da sua emissão.

12.2.3. Para efeito de julgamento das propostas eletrônicas, o valor a ser informado no sistema eletrônico, pelas licitantes situadas no Estado do Ceará, será o valor deduzido do percentual de 7,5% (sete inteiros e cinco décimos por cento) para os itens 9, 10 e 11 do grupo 1, correspondente à média das diferenças de alíquotas interestaduais do ICMS, nos termos do disposto no Decreto Estadual nº 27.624/2004.

12.2.3.1. A dedução acima referida não se aplica ao fornecimento de produtos isentos e não tributados, e, na hipótese de a alíquota interna ser inferior ao percentual de 7,5% (sete inteiros e cinco décimos por cento), devendo, neste caso, ser aplicado o percentual correspondente à alíquota cobrada.

12.3. As licitantes poderão retirar ou substituir as propostas e os documentos de habilitação por eles apresentadas, até o término do prazo para recebimento.

12.4. Somente serão aceitas a realização de cotações, por fornecedor, que representem 100% (cem por cento) das quantidades demandadas.

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

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

12.7. Os documentos de habilitação deverão ser apresentados da seguinte forma:

12.7.1. Obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos tanto para matriz como para todas as filiais. O contrato será celebrado com a sede que apresentou a documentação.

12.7.2. O documento obtido através de *sítios* oficiais, que esteja condicionado à aceitação via internet, terá sua autenticidade verificada pelo pregoeiro.

12.7.3. Todos os documentos emitidos em língua estrangeira deverão ser acompanhados da tradução para língua portuguesa, efetuada por tradutor juramentado, e também consularizados ou registrados no cartório de títulos e documentos.

12.7.3.1. Documentos de procedência estrangeira, emitidos em língua portuguesa, também deverão ser apresentados consularizados ou registrados em cartório de títulos e documentos.

12.7.4. Dentro do prazo de validade. Na hipótese de o documento não constar expressamente o prazo de validade, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. Na ausência de tal declaração ou regulamentação, o documento será considerado válido pelo prazo de 90 (noventa) dias, contados a partir da data de sua emissão, quando se tratar de documentos referentes à habilitação fiscal e econômico-financeira.

13. DA ABERTURA E ACEITABILIDADE DAS PROPOSTAS ELETRÔNICAS

13.1. Abertas as propostas, o pregoeiro fará as devidas verificações, avaliando a aceitabilidade das mesmas. Caso ocorra alguma desclassificação, deverá ser fundamentada e registrada no sistema.

13.2. Os preços deverão ser expressos em reais, com até 2 (duas) casas decimais em seus valores globais.

13.3. O sistema ordenará automaticamente as propostas classificadas pelo pregoeiro e somente estas participarão da etapa de lances.

14. DA ETAPA DE LANCES

14.1. O pregoeiro dará início à etapa competitiva no horário previsto no subitem 6.3., quando, então, as licitantes poderão encaminhar lances.

14.2. Para efeito de lances, será considerado o VALOR UNITÁRIO DO ITEM.

14.3. Aberta a etapa competitiva, será considerado como primeiro lance a proposta inicial. Em seguida as licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo a licitante imediatamente informada do seu recebimento e respectivo horário de registro e valor.

14.4. As licitantes poderão ofertar lances sucessivos, desde que inferiores ao seu último lance registrado no sistema, ainda que este seja maior que o menor lance já ofertado por outra licitante.

14.4.1. Em caso de dois ou mais lances de igual valor, prevalece aquele que for recebido e registrado em primeiro lugar.

14.5. Durante a sessão pública de disputa, as licitantes serão informadas, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances ao pregoeiro nem as demais participantes.

14.6. Será adotado para o envio de lances o modo de disputa "ABERTO E FECHADO", em que as licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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

14.8. Encerrado o prazo previsto no item 14.7., o sistema abrirá oportunidade para que a licitante da oferta de valor mais baixo e os das ofertas com preços até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

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

14.9. Após o término dos prazos estabelecidos, o sistema ordenará os lances segundo a ordem crescente de valores.

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

14.10. Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhuma licitante classificada na etapa de lance fechado atender às exigências de habilitação.

14.11. No caso de desconexão entre o pregoeiro e o sistema no decorrer da etapa competitiva, o sistema poderá permanecer acessível à recepção dos lances, retornando o pregoeiro, quando possível, sem prejuízos dos atos realizados.

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

14.13. Após o encerramento dos lances, o sistema detectará a existência de situação de empate ficto. Em cumprimento ao que determina a Lei Complementar nº 123/2006, a microempresa, a empresa de pequeno porte e a cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007, e que ofertou lance de até 5% (cinco por cento) superior ao menor preço da arrematante que não se enquadre nessa situação de empate, será convocada automaticamente pelo sistema, na sala de disputa, para, no prazo de 5 (cinco) minutos, utilizando-se do direito de preferência, ofertar novo lance inferior ao melhor lance registrado, sob pena de preclusão.

14.13.1. Não havendo manifestação da licitante, o sistema verificará a existência de outra em situação de empate, realizando o chamado de forma automática. Não havendo outra situação de empate, o sistema emitirá mensagem.

14.14. O sistema informará a proposta de menor preço ao encerrar a fase de disputa.

15. DA LICITANTE ARREMATANTE

15.1. O pregoeiro poderá negociar exclusivamente pelo sistema, em campo próprio, a fim de obter melhor preço.

15.2. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta a licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.
15.3. Definido o valor final da proposta, o pregoeiro convocará a arrematante para anexar em campo próprio do sistema, no prazo de até 24 (vinte e quatro) horas, a proposta de preços com os respectivos valores readequados ao último lance ofertado.087794512019

15.3.1. A proposta deverá ser anexada em conformidade com todo o item 12.2. deste edital.

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

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

15.6. O descumprimento dos prazos acima estabelecidos é causa de desclassificação da licitante, sendo convocada a licitante subsequente, e assim sucessivamente, observada a ordem de classificação.

15.7. Nos termos do Decreto Estadual nº 27.624/2004, a arrematante situada no Estado do Ceará deverá apresentar para os itens 9,10 e 11 do grupo 1, a proposta com o valor acrescido do diferencial referido no subitem 12.2.3, mediante a utilização da seguinte fórmula:

$$VFP = \frac{VPV}{0{,}925}$$

Onde:
VFP = Valor Final da Proposta, acrescido da alíquota de 7,5% (sete inteiros e cinco décimos por cento);

VPV = Valor da Proposta Vencedora após o encerramento da disputa eletrônica anunciado pelo sistema;

0,925 = Fator de Reversão correspondente a 7,5% (sete inteiros e cinco décimos por cento), que foram deduzidos antes da disputa.

15.8. Para efeito de cálculo será observado o previsto no subitem 12.2. deste edital.

15.9. Após a apresentação da proposta não caberá desistência.

16. DOS CRITÉRIOS DE JULGAMENTO

16.1. Para julgamento das propostas será adotado o critério de MENOR PREÇO POR GRUPO, observado o estabelecido no Decreto Estadual nº 27.624/2004 para os itens 9,10, 11 e todas as condições definidas neste edital.

16.1.1. A disputa será realizada POR GRUPO, sendo os preços registrados em Ata, pelo valor unitário do item.

16.1.2. A proposta final para o grupo não poderá conter item com valor superior ao estimado pela administração, sob pena de desclassificação, independente do valor total do grupo.

16.2. Se a proposta de menor preço não for aceitável, ou, ainda, se a licitante desatender às exigências habilitatórias, o pregoeiro examinará a proposta subsequente, verificando sua compatibilidade e a habilitação da participante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda a este edital.

16.3. A licitante remanescente que esteja enquadrada no percentual estabelecido no art. 44, § 2º, da Lei Complementar nº 123/2006, no dia e hora designados pelo pregoeiro, será convocada para na sala de disputa, utilizar-se do direito de preferência, ofertando no prazo de 5 (cinco) minutos, novo lance inferior ao melhor lance registrado no item.

16.4. Serão desclassificadas as propostas:

16.4.1. Contenham vícios insanáveis.

16.4.2. Descumpram especificações técnicas constantes do instrumento convocatório.

16.4.3. Apresentem preços manifestamente inexequíveis.

16.4.4. Se encontrem acima do orçamento estimado para a contratação após encerrada a negociação de menor preço.

16.4.5. Não tenham sua exequibilidade demonstrada, quando exigido pela ETICE.

16.4.6. Apresentem desconformidade com outras exigências do instrumento convocatório, salvo se for possível a acomodação a seus termos antes da adjudicação do objeto e sem que se prejudique a atribuição de tratamento isonômico entre as licitantes.

16.5. A ETICE poderá realizar diligências para aferir a exequibilidade das propostas ou exigir das licitantes que ela seja demonstrada.

16.6. A desclassificação será sempre fundamentada e registrada no sistema.

17. DOS RECURSOS ADMINISTRATIVOS

17.1. Qualquer licitante poderá manifestar, de forma motivada, a intenção de interpor recurso, em campo próprio do sistema, no prazo de até 20 minutos depois da arrematante ser aceita e habilitada, quando lhe será concedido o prazo de 3 (três) dias para apresentação das razões do recurso no sistema Comprasnet. As demais licitantes ficam desde logo convidados a apresentar contrarrazões dentro de igual prazo, que começará a contar a partir do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

17.1.1. Para abertura da manifestação da intenção de recurso, o pregoeiro comunicará a retomada da sessão pública com no mínimo vinte e quatro horas de antecedência, no sítio eletrônico utilizado para realização do certame.

17.2. Não serão conhecidos os recursos intempestivos e/ou subscritos por representante não habilitado legalmente ou não identificado no processo licitatório para responder pelo proponente.

17.3. A falta de manifestação, conforme o subitem 17.1. deste edital, importará na decadência do direito de recurso.

17.4. O acolhimento de recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

17.5. A decisão em grau de recurso será definitiva, e dela dar-se-á conhecimento as licitantes, no endereço eletrônico constante no subitem 5.2. deste edital.

18. DA HOMOLOGAÇÃO E DA ASSINATURA DA ATA DE REGISTRO DE PREÇOS

18.1. O sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

18.2. A homologação se dará na forma do inciso IV do art. 12 do Decreto Estadual n° 33.326/2019.

18.3. Após a homologação do resultado da licitação, os preços ofertados pelas licitantes vencedoras dos itens, serão registrados na Ata de Registro de Preços, elaborada conforme o Anexo III, deste edital.

18.3.1. As licitantes classificadas em primeiro lugar terão o prazo de 5 (cinco) dias úteis, a contar da data do recebimento da convocação, para comparecerem perante o gestor a fim de assinarem a Ata de Registro de Preços, sob pena de decair do direito à contratação, e sem prejuízo das sanções previstas no Edital, podendo o prazo de comparecimento ser prorrogado uma vez, por igual período, desde que ocorra motivo justificado e aceito pela administração.

18.4. A Ata de Registro de Preços poderá ser assinada por certificação digital.

18.5. Homologada a licitação e obedecida a sequência da classificação do certame, as licitantes serão convocadas, por meio do sistema eletrônico, para no prazo de 2 (dois) dias úteis, se assim desejarem, ajustarem seus preços ao valor da proposta da licitante mais bem classificada, visando a formação de cadastro de reserva.

18.5.1. As licitantes que aderiram ao cadastro de reserva obedecerão ao disposto no subitem 18.3.1. deste edital.

18.6. É facultado à Administração após a homologação da licitação e desde que, obedecido a ordem de classificação, convocar as licitantes remanescentes para assinarem a ata de registro de preços, em igual prazo e nas mesmas condições propostas pela vencedora, quando esta não atender a convocação, ou no caso da exclusão do detentor de preço registrado, nas hipóteses previstas no art. 25 do Decreto Estadual n.º 32.824/2018.

18.6.1. Ocorrido o disposto no subitem 18.6. deste edital, respeitada a ordem de classificação, o pregoeiro convocará as licitantes do cadastro de reserva para comprovar as condições de habilitação e proposta compatível com o objeto licitado. Não havendo cadastro de reserva o pregoeiro convocará as demais remanescentes desde que realizada a negociação nas mesmas condições de habilitação e proposta da licitante vencedora. Após habilitada e classificada a licitante obedecerá o disposto no subitem 18.3.1. deste edital.

18.7. O prazo de validade da ata de registro de preços, computadas as eventuais prorrogações, não poderá ser superior a doze meses, contado a partir da data da sua publicação.

18.8. A licitante vencedora fica obrigada a apresentar no ato da assinatura do contrato, o Certificado de Registro Cadastral - CRC emitido pela Secretaria de Planejamento e Gestão do Estado do Ceará.

19. DAS SANÇÕES ADMINISTRATIVAS

19.1. A licitante que praticar quaisquer das condutas previstas no art. 37, do Decreto Estadual nº 33.326/2019, sem prejuízo das sanções legais nas esferas civil e criminal, inclusive as decorrentes da Lei nº 12.846/2013, estará sujeita às seguintes penalidades:

19.1.1. Multa de 10% (dez por cento) sobre o valor da proposta.

19.1.2. Impedimento de licitar e contratar com a Administração, sendo, então, descredenciado no cadastro de fornecedores da Secretaria do Planejamento e Gestão (SEPLAG), do Estado do

Ceará, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo da multa prevista neste edital e das demais cominações legais.

19.2. A ETICE dará publicidade da sanção administrativa para registro no Cadastro de Fornecedores do Estado.

19.3. A licitante recolherá a multa por meio de depósito bancário em nome da ETICE, Se não o fizer, será cobrada em processo de execução.

20. DA ATA DE REGISTRO DE PREÇOS

20.1. A Empresa da Tecnologia da Informação do Ceará - ETICE será o órgão gestor da Ata de Registro de Preços de que trata este edital.

20.2. A Ata de Registro de Preços que tem caráter convocatório, elaborada conforme o anexo III, será assinada pelo titular da Empresa da Tecnologia da Informação do Ceará - ETICE, órgão gestor do Registro de Preços ou, por delegação, por seu substituto legal, e pelos representantes de cada um dos prestadores de serviços legalmente credenciados e identificados.

20.3. Os preços registrados na Ata de Registro de Preços serão aqueles ofertados nas propostas de preços das licitantes vencedoras e das demais interessadas em praticar os mesmos valores e condições da vencedora, conforme inciso III do art. 11 do Decreto nº 32.824/2018.

20.4. A Ata de Registro de Preços uma vez lavrada e assinada, não obriga a Administração a firmar as contratações que dela poderão advir, ficando-lhe facultada a utilização de procedimento de licitação, respeitados os dispositivos da Lei Federal 13.303/2016, sendo assegurado ao detentor do registro de preços a preferência em igualdade de condições.

20.5. A Empresa da Tecnologia da Informação do Ceará - ETICE, na condição de único participante do SRP (Sistema de Registro de Preços) quando necessitar, efetuará os serviços junto aos prestadores de serviços detentores de preços registrado087794512019s na Ata de Registro de Preços, de acordo com as especificações e quantitativos previstos, durante a vigência do documento supracitado.

20.6. Os prestadores de serviços detentores de preços registrados ficarão obrigados a executar o objeto licitado ao participante do SRP(Sistema de Registro de Preços), nos prazos, locais, quantidades e, demais condições definidas no Anexo I - Termo de Referência deste edital.

20.7. A Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por **órgão** ou entidade de outros entes federativos, como órgão interessado, mediante consulta prévia ao órgão gestor do registro de preços, conforme disciplina os artigos 19, 20, 21 e 22 do Decreto Estadual nº 32.824/2018.

20.8. Os órgãos interessados, quando desejarem fazer uso da Ata de Registro de Preços, deverão manifestar seu interesse junto ao órgão gestor do Registro de Preços, o qual indicará o prestador de serviço e o preço a ser praticado.

20.8.1. As contratações decorrentes da utilização da Ata de Registro de Preços de que trata este subitem não poderão exceder, por órgão Interessado, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços.

20.8.2. O quantitativo decorrente das adesões à Ata de Registro de Preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços, independente do número de órgãos interessados que aderirem.

20.8.3. O órgão interessado deverá efetivar a aquisição ou contratação solicitada em até noventa dias, contados a partir da autorização do órgão gestor do registro de preços, observado o prazo de vigência da ata.

20.8.4. A comunicação ao gestor do registro de preços acerca do cumprimento do prazo previsto no item 20.8.3. será providenciada pelo órgão interessado até o quinto dia útil após a aquisição ou contratação.

20.8.5. O órgão gestor do registro de preços não autorizará a adesão à ata de registro de preços para contratação separada de itens de objeto adjudicado por preço global para os quais o fornecedor não tenha apresentado o menor preço.

20.9. Caberá ao órgão gestor do Registro de Preços, para utilização da Ata por órgãos interessados da Administração Pública, proceder a indicação do prestador de serviço detentor do preço registrado, obedecida a ordem de classificação.

20.10. O detentor de preços registrados que descumprir as condições da Ata de Registro de Preços nos termos previstos nos incisos I a VIII do artigo 25 do decreto 32.824/2018 terá o seu registro cancelado.

20.11. Os preços registrados poderão ser revistos a qualquer tempo em decorrência da redução dos preços praticados no mercado ou de fato que eleve os custos dos itens registrados, obedecendo aos parâmetros constantes no art. 23, do Decreto Estadual n.º 32.824/2018.

20.12. A ETICE convocará o prestador para negociar o preço registrado e adequá-lo ao preço de mercado, sempre que verificar que o preço registrado está acima do preço de mercado. Caso seja frustrada a negociação, o prestador de serviço será liberado do compromisso assumido.

20.13. Não havendo êxito nas negociações com os prestadores de serviços com preços registrados, o gestor da Ata, poderá convocar os demais prestadores de serviços classificados, podendo negociar os preços de mercado, ou cancelar o item, ou ainda revogar a Ata de Registro de Preços.

20.14. Serão considerados preços de mercado, os preços que forem iguais ou inferiores à média daqueles apurados pela Administração para os itens registrados.

20.15. As alterações dos preços registrados, oriundas de revisão dos mesmos, serão publicadas no Diário Oficial do Estado e na página oficial do Governo do Estado na internet.

20.16. As demais condições contratuais se encontram estabelecidas no Anexo IV- Minuta do Contrato.

20.17. Os serviços previstos no Anexo I - Termo de Referência deste edital, são estimativas máximas para o período de validade da Ata de Registro de Preços, reservando-se a Administração, através do órgão participante, o direito de executá-los no quantitativo que julgar necessário ou mesmo abster-se do executar o item especificado.

20.18. DA GARANTIA CONTRATUAL

20.18.1. Após a homologação do objeto do certame e até a data da contratação, a licitante vencedora deverá prestar garantia contratual correspondente a 5% (cinco por cento) sobre o valor do contrato, em conformidade com o disposto no art. 70, da Lei Federal nº 13.303/2016, vedada à prestação de garantia através de Título da Dívida Agrária.

20.18.2. Na garantia deverá estar expresso prazo de validade superior a 90 (noventa) dias do prazo contratual.

20.18.3. A não prestação de garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a licitante sujeito às penalidades legalmente estabelecidas, inclusive multa.

20.19. DA SUBCONTRATAÇÃO

20.19.1. Será admitida a subcontratação no limite de 30% (trinta por cento) do objeto, conforme disposto no art. 78 da Lei nº 13.303/2016, desde que não constitua o escopo principal da contratação, e, se previamente aprovada pela ETICE.

20.19.2. A subcontratação de que trata esta cláusula, não exclui a responsabilidade da contratada perante a ETICE quanto à qualidade do objeto contratado, não constituindo portanto qualquer vínculo contratual ou legal da ETICE com a subcontratada.

20.19.3. A contratada ao requerer autorização para subcontratação de parte do objeto, deverá comprovar perante a Administração a regularidade jurídico/fiscal e trabalhista de sua subcontratada.

21. DA FRAUDE E DA CORRUPÇÃO

21.1. As licitantes devem observar e a contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos deste item, definem-se as seguintes práticas:

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

b) “prática fraudulenta”: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato.

c) “prática conluiada”: esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos.

d) “prática coercitiva”: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando a influenciar sua participação em um processo licitatório ou afetar a execução do contrato.
e) “prática obstrutiva”:
(1) Destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista neste subitem.

(2) Atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

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

21.3. Considerando os propósitos dos itens acima, a licitante vencedora como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou

reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

21.4. A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas em lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

22. DAS DISPOSIÇÕES GERAIS

22.1. Esta licitação não importa necessariamente em contratação, podendo a autoridade competente revogá-la por razões de interesse público, anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante decisão devidamente fundamentada, sem quaisquer reclamações ou direitos à indenização ou reembolso.

22.2. É facultada ao pregoeiro ou à autoridade competente, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos que deveriam constar originariamente na proposta e na documentação de habilitação.

22.3. O descumprimento de prazos estabelecidos neste edital e/ou pelo pregoeiro ou o não atendimento às solicitações ensejará DESCLASSIFICAÇÃO ou INABILITAÇÃO.

22.4. Toda a documentação fará parte dos autos e não será devolvida a licitante, ainda que se trate de originais.

22.5. Na contagem dos prazos estabelecidos neste edital, excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. Os prazos estabelecidos neste edital para a fase externa se iniciam e se vencem somente nos dias e horários de expediente da Central de Licitações. Os demais prazos se iniciam e se vencem exclusivamente em dias úteis de expediente da contratante.

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

22.7. O desatendimento de exigências formais não essenciais não implicará no afastamento da licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

22.8. Caberá a licitante acompanhar as operações no sistema eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

22.9. O pregoeiro poderá sanar erros formais que não acarretem prejuízos para o objeto da licitação, a Administração e as licitantes, dentre estes, os decorrentes de operações aritméticas.

22.10. Os casos omissos serão resolvidos pelo pregoeiro, nos termos da legislação pertinente.

22.11. As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa.

22.12. O foro designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da Comarca de Fortaleza, Capital do Estado do Ceará.

23. DOS ANEXOS

23.1. Constituem anexos deste edital, dele fazendo parte:

ANEXO I - TERMO DE REFERÊNCIA

ANEXO II - CARTA PROPOSTA

ANEXO III - MINUTA DA ATA DE REGISTRO DE PREÇOS

ANEXO IV - MINUTA DO CONTRATO

ANEXO V - MODELO DE DECLARAÇÃO DE AUTENTICIDADE DOS DOCUMENTOS (Anexar com a documentação de habilitação)

Fortaleza - CE, 23 de dezembro de 2019.

CIENTE:

_____	_____
Adalberto Albuquerque de Paula Pessoa	Raimundo Vieira Coutinho
ORDENADOR DE DESPESA	PREGOEIRO

Aprovado:_____

(aprovação da assessoria ou procuradoria jurídica conforme o caso)

ANEXO I - TERMO DE REFERÊNCIA

1. UNIDADE REQUISITANTE: ETICE / DITEC

2. DO OBJETO:

Registro de preços para futuras e eventuais **serviços de fornecimento, aquisição, manutenção de Solução Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Empresa de Tecnologia da Informação do Ceará**, de acordo com as especificações e quantitativos previstos neste Termo.

2.1.Este objeto será realizado através de licitação na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO, sob o regime de execução indireta: Empreitada por preço unitário.

3. DA JUSTIFICATIVA:

3.1. A missão institucional da Empresa de Tecnologia da Informação do Ceará – ETICE é fortalecer a gestão pública e o desenvolvimento econômico e social, por meio da Tecnologia da Informação e Comunicação (TIC), consoante o disposto do art. 5º do Decreto nº. 32.792, publicado no Diário Oficial do Estado de 23 de agosto de 2018.

A Lei nº 16.727, de 26 de dezembro de 2018, instituiu, no âmbito interno da administração pública do Estado do Ceará, o programa Hub de Tecnologia da Informação e Comunicação (HTIC), visando otimizar, de forma contínua, os recursos de custeio e investimentos em TIC (Tecnologia de Informação e Comunicação), compartilhar recursos de TIC entre os órgãos/entidades da administração, prover novas tecnologias para atender às demandas requeridas pelo serviço público, disponibilizar links de dados e internet de alta velocidade, com qualidade, às unidades administrativas e à população do Estado e fomentar o crescimento econômico no segmento de TIC dentro do Estado.

O programa HTIC vem favorecer o estabelecimento de padrões de interoperabilidade no estado, gerando economia em escala, maior segurança e confiabilidade dos dados públicos, estando em estrita sintonia com a política do Governo do Ceará, sendo oportuna a formatação de um hub tecnológico no estado em decorrência da excelente posição geográfica do Ceará e por concentrar o tráfego de 13 (treze) cabos submarinos que chegam à capital cearense oriundos dos EUA, Europa e África e que estão atraindo grandes datacenters a nossa região.

Para a consecução dos objetivos previstos no programa HTIC, caberá, com exclusividade, à Empresa de Tecnologia da Informação do Ceará – ETICE, a responsabilidade de execução, direta ou indiretamente (através de parcerias, convênios, contratos com empresas terceirizadas ou demais instrumentos), dos serviços relacionados no Capítulo II da Lei nº 16.727, conforme artigos listados a seguir:

A ETICE, vem investindo em seu ambiente tecnológico visando assegurar a qualidade dos diversos serviços prestados, bem como manter o seu portfólio de serviços cada vez mais completo, a fim de atender as necessidades e demandas de TI que venham existir em todos os órgãos da administração direta e indireta do Estado.

A Etice tem a perspectiva de atuar como um instrumento de modernização e fortalecimento da governança, através de ações vanguardistas e inovadoras em TIC, visando contribuir para um Estado eficiente, justo e transparente.

A modernização tecnológica para atendimento das crescentes necessidades do mercado, evidenciada pelo contínuo desenvolvimento de novas soluções, com maior necessidade de recursos de Segurança da Informação, pode ocasionar a obsolescência tecnológica e tem como efeito a descontinuidade de equipamentos, componentes ou licenças, elevando o custo de manutenção de uma tecnologia legada e em alguns casos, inviabilizando sua utilização. Nesta perspectiva, no âmbito Governamental, investimentos de atualizações TIC deixam de ser uma opção, passando a ser mandatórios, quando considerado o compromisso de assegurar a eficiência na gestão do Estado e o atendimento das necessidades dos cidadãos.

Tendo em vista a constância dessas atualizações e investimentos em função da obsolescência, cabe aos gestores governamentais, o pensar estratégico, não só quanto ao uso da TIC como diferencial de sustentabilidade e gestão, mas também, quanto à aplicação eficiente dos investimentos de forma a reduzir a suscetibilidade do estado à obsolescência tecnológica.

Para o Governo do Estado do Ceará, planejar com inteligência as ações na área de Tecnologia da Informação, alinhando redução de custos com a garantia de maior eficiência para gestão governamental e, por consequência, o atendimento às expectativas da população, constitui um dos grandes diferenciais da sua atuação e corrobora para a aprovação dos cidadãos. E assim sendo, as normatizações estaduais relativas aos procedimentos de planejamento e aquisição de bens e serviços de TIC, estão pautadas na otimização dos recursos, fomentando o uso compartilhado da Segurança da Informação.

A contratação em questão busca promover a padronização, aquisição e manutenção contínua da infraestrutura de TI, a qual tem como necessidade adquirir soluções de segurança vinculando-se com a estratégia da ETICE, onde os objetivos estratégicos visam desenvolver, implantar, manter e evoluir aplicações, promovendo a gestão da informação e de processos institucionais e a padronização.

Ao longo dos últimos anos houve um considerável crescimento no número de ataques às redes de dados corporativas, observando-se também a diversificação tanto da metodologia de ataque quanto da forma de disseminação, gerando vários efeitos e prejuízos.

Conforme amplamente divulgado pela imprensa especializada, o índice de sucesso alcançado tem sido bastante alto e até mesmo grandes corporações têm se ressentido de tais ataques.

As organizações especializadas em segurança têm sido unânimes em suas recomendações e ações no sentido de que a melhor forma de defesa é a integração das várias ferramentas disponíveis, criando-se desta forma um conjunto de barreiras capazes de detectar em tempo hábil qualquer forma de ataque, conhecida ou não, e ao mesmo tempo impedir a sua propagação em paralelo.

A ETICE tem a responsabilidade de manter íntegro, confiável e seguro todo o ambiente tecnológico, bem como manter e disponibilizar, à sociedade e aos servidores, equipamentos, bases de dados e informações precisas e confiáveis.

No âmbito da lei nº 13.709/2018 – LGPD, os dados pessoais são informações relativas à pessoa física que possa ser identificada com apenas uma informação podendo também ser identificada com o cruzamento de duas ou mais informações, já a manipulação dos dados é toda operação realizada com os dados pessoais, sendo ela a coleta, utilização, remoção e/ou transferência destes dados.

A proteção aos princípios da privacidade e da intimidade já estão garantidos e observados no direito brasileiro, no entanto, a legislação não acompanhou o avanço tecnológico, com isso garantir tais princípios se tornou um desafio praticamente intransponível sem o auxílio da tecnologia.

A LGPD busca não apenas alinhar estes novos requisitos a partir da implementação de diretrizes, obrigações, direitos aos titulares, imposição de fiscalização e aplicação de sanções, retomando um pouco da segurança jurídica, mas possibilitando também a criação de novas culturas para o povo e instituições relacionadas ao tratamento de dados pessoais e sua privacidade.

A LGPD aplica-se tanto para pessoas físicas quanto jurídicas seja nos meios físicos e virtuais, nos âmbitos público e privado, atendendo ao menos um dos seguintes requisitos:

I – Possuam estabelecimento no Brasil;

II – Ofereçam serviços ao mercado consumidor brasileiro; e/ou

III – Coletem e tratem dados de pessoas localizadas no Brasil.

Dentre as diversas orientações e obrigações a lei nº 13.709/2018 – LGPD, implementa pontos de suma importância como intuito de estabelecer uma segurança jurídica nas relações referentes ao tratamento dos dados. Em linhas gerais pode-se estabelecer padrões e princípios que orientam quanto os dados pessoais (Art. 2º), assim como, define “o que são” dados pessoais (Art. 5º), em específico dados sensíveis (Art. 11), elencando os pré-requisitos básicos para o tratamento (Art. 7º), implementando regras e definindo sobre a localidade do tratamento dos dados (Art. 3º) e abordando sobre o término do tratamento dos dados (Art. 15), o que implementa minimamente quais são os dados pessoais e requisitos gerais para seu tratamento.

No entanto, a LGPD trata ainda, no Art. 17, quanto aos direitos do titular, já no Art. 23 estabelece quanto ao tratamento de dados pelo Poder Público e, por conseguinte nos Art. 25 e 33 estabelecendo as responsabilidades e do trato na transferência internacional de dados, tais marcos são vitais para segurança jurídica das atividades digital, uma vez que em sua grande maioria os grandes fornecedores de nuvens públicas são empresas globais, com presenças em diversos países. A LGPD é permeada de responsabilidades e responsáveis, implementando obrigações e responsabilidades, que são outros aspectos importantes na busca de segurança jurídica.

Percebe-se ainda que o Art. 46 em sua totalidade em conjunto com o Art. 50 trata-se especificamente da segurança e das boas práticas envolvendo dados, inclusive determinando que medidas de privacidade devem ser observadas do início ao fim, ou seja, desde sua criação à implementação e execução, da mesma forma que dispõem sobre boas práticas de governança e conformidade no âmbito digital (§2º, I e II).

A partir do Art. 52 a LGPD trata das sanções administrativas, direcionando desta forma, quais as consequências caberão com o descumprimento de algum dos itens, as quais serão impostas pela Autoridade Nacional de Proteção de Dados prevista no Art. 55 e do Conselho Nacional de Proteção de Dados a partir do Art. 58 que serão responsáveis por fiscalizar e orientar as políticas relacionadas à proteção de dados pessoais, sendo responsáveis também por intermediar a relação entre o usuário e órgão.

Baseada nestas orientações supracitadas, a ETICE, ciente que hoje a superfície de ataque está exponencialmente maior que a poucos anos atrás, com a adoção dos ambientes em nuvem, onde a gestão dos dados torna-se uma tarefa muito mais penosa e desafiadora, e onde o atacante não tem compromisso com o acerto, pois, em sua perspectiva errônea “não estão sujeitos as sanções”, e ainda na busca por atender na íntegra os requisitos da lei, evitando as possíveis penalidades que podem advir oriundos de um ataque à rede governamental, seja com o objetivo meramente de negação de serviço da rede de comunicação de dados, seja por objetivos mais perniciosos de roubo ou destruição de informações, sendo assim, foi definido como prioridade a adoção de uma camada de tecnologia robusta com o intuito de cobrir as áreas de Segurança de Dados,

Monitoração do Uso dos Dados, Prevenção Contra o Vazamento dos Dados nos ambientes locais e em nuvem.

Para isso foi determinada a imediata disponibilização de ata de registro de preços das tecnologias de proteção de acesso web a partir de um Gateway de Segurança Web, Serviço de Proxy em Nuvem, Solução para Acesso Seguro em Ambiente de Nuvem, proteção das estações de trabalho e servidores a partir de soluções para Proteção de Estação de Trabalho e Servidores, Solução para Prevenção de Ataques Direcionados e Avançados, Segurança para Dispositivos Móveis, Solução para Proteção de Dados em Servidores Críticos, Conformidade e Legados, proteção das comunicações tratadas pelo meio digital via serviço de e-mail a partir de tecnologias de Segurança de Mensageria, Segurança de Mensageria em Nuvem, Segurança de Correio Eletrônico, proteção e contextualização do uso dos dados a partir de tecnologias para Proteção, Monitoramento e Descoberta de Dados Confidenciais, Proteção, Monitoramento e Descoberta de Dados Confidenciais em Nuvem, Solução de Manutenção do Sigilo e Integridade da Informação, proteção, monitoração e visibilidade de tráfego cifrado e de tecnologias já implementadas possibilitando um upgrade nos níveis de segurança com a integração das soluções a serem integradas, assim como, com as tecnologias já existentes no Órgão.

A partir da adoção das tecnologias de Solução para Inspeção de SSL e Solução Remota de Monitoramento e Gerência da Segurança, fornecendo um ambiente de segurança integrado, com uma visibilidade única, resposta a incidentes e tomada de ações automatizadas minimizando o tempo de resposta e posicionamento, a partir de uma Solução de Gerenciamento com ação ampla, implementando-se desta forma, um sistema de defesa mais amplo contemplando também a proteção contra as mais diversas outras formas de ataque, atuando de forma integrada e padronizada, além, da possibilidade de ampliação das funcionalidades técnicas e de operação com a integração entre as tecnologias.

A arquitetura da solução de Segurança da Informação a ser adquirida está focada nas melhores práticas de segurança e em conformidade com a Lei Geral de Proteção de Dados – LGPD (lei nº 13.709/2018) e nas melhores ferramentas disponíveis no mercado para a segurança de ambientes corporativos. Além dos benefícios inerentes aos novos sistemas, quanto ao aspecto de desempenho e alta disponibilidade, possuem agregado outras funcionalidades que permitirão à equipe de informática do órgão fazer melhor gestão dos recursos computacionais e agir proativamente em situações de risco e infestação.

Diante do exposto, torna-se necessário e urgente proteger os dados e eliminar o risco de perda dos dados sob responsabilização pela Lei Geral de Proteção de Dados e demais dispositivos legais e jurisprudências, através da disponibilização de ata de registro de preços de solução integrada de proteção de dados, visando adaptação em conformidade Lei.

- Aumento da segurança através das integrações das soluções;
- Várias camadas de proteção em segurança de endpoints, mensageria e Internet, prevenção contra a perda de dados e recuperação de dados e sistemas;
- Eliminar a complexidade do ambiente através da implementação de tecnologias de segurança de endpoints e da mensageria essenciais integradas, como soluções unificadas com gerenciamento coordenado;
- Controles automáticos ajudam você a obter, provar e aplicar políticas de TI e objetivos regulamentares com facilidade;
- Implementação e operações simplificadas com rápida implementação e mínimo de interrupção em seu ambiente, através do gerenciamento fácil e do uso otimizado dos recursos do sistema.

• Proteção de endpoint abrangente contra ameaças maliciosas direcionadas aos sistemas operacionais Windows, Linux, Macintosh, iOS, Android.

• A solução integrada amplia o número e a intensidade das defesas em face da exponencial curva crescente de complexidade dos ataques e vulnerabilidades e, por ser integrada, racionaliza o controle e a administração resultando numa maior eficiência.

• Gerar relatórios avançados e métricas gerenciais, a solução de segurança e os demais módulos utilizando a mesma inteligência de gerenciamento, são capazes de prover visibilidade sobre as diversas ameaças e correlacioná-las com a rede de inteligência global e provendo a integração de suas ferramentas de segurança, garantindo console única de manutenção, alerta e mitigação de eventos de segurança.

• O uso de uma mesma console e agente para todas as funcionalidades relacionadas acima facilita operações anteriormente conhecidas como complexas ou demoradas, automatizando esforços e trazendo melhorias operacionais, reduzindo investimento com hardwares e softwares para soluções isoladas, aproveitando melhor recursos.

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoas. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Desta forma a segurança da informação abrange, dentre outros meios, a implementação de mecanismos de segurança no que se refere a controles lógicos.

Ressalta-se que a Missão da ETICE é fortalecer a gestão pública e o desenvolvimento econômico e social, por meio da Tecnologia da Informação e Comunicação (TIC).

Prezando pela melhoria da qualidade dos serviços prestados a seus usuários internos e externos, além do contínuo aperfeiçoamento de Governança de TI, especialmente no tocante ao crucial tema da segurança da informação, aponta-se como essencial ao adequado funcionamento de sua estrutura tecnológica a implementação de uma Solução de Segurança, Proteção e Monitoramento da Informação eficiente e que contemple o quantitativo total dos usuários e dispositivos dos Órgãos.

Portanto, é tecnicamente viável e extremamente necessária a disponibilização de ata de registro de preços de solução de segurança da informação, cujo investimento futuro fortalecerá prontamente a capacidade e eficiência do Governo do Estado no cumprimento efetivo de suas ações e competências legais.

Somando ao exposto, a disponibilização de ata de registro de preços de solução de segurança poderá permitir e impulsionar a integração de diversas informações em uma única plataforma colaborativa para alcançar diferentes perspectivas de gestão, visando agilizar a tomada de decisão, dar transparência e aumentar a qualidade da gestão.

Pelo exposto, não restam dúvidas quanto à necessidade e legalidade do estabelecimento de uma ata de registro de preços de soluções de segurança da informação, uma vez que, amparados em motivos de ordem técnicas, ficou demonstrado que na hipótese, se mostra mais vantajoso para a administração tornar o parque padronizado e integrado, amparados pelos termos da Lei.

4. DAS ESPECIFICAÇÕES E QUANTITATIVOS

GRUPO 1 – Serviços de fornecimento, aquisição, manutenção de Solução Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Empresa de Tecnologia da Informação do Ceará			
Item	**Descrição**	**Qtde**	**Unidade de Medida**
1	Fornecimento de licenças de uso de solução corporativa de antivírus, anti-exploit/anti-ransomware para estações de trabalho com gerência em nuvem. COMPRASNET: UNIDADE = LICENÇA	5000	Licença
2	Fornecimento de licenças de uso de solução corporativa de antivírus de anti-exploit/anti-ransomware para servidores com gerência em nuvem. COMPRASNET: UNIDADE = LICENÇA	500	Licença
3	Fornecimento de licenças de criptografia de arquivos de rede. COMPRASNET: UNIDADE = LICENÇA	5000	Licença
4	Fornecimento de licenças de criptografia de discos. COMPRASNET: UNIDADE = LICENÇA	5000	Licença
5	Fornecimento de licenças de criptografia para mídias removíveis. COMPRASNET: UNIDADE = LICENÇA	5000	Licença
6	Fornecimento de licenças de criptografia de dados na nuvem. COMPRASNET: UNIDADE = LICENÇA	5000	Licença
7	Fornecimento de licenças de uso de solução de controle de dispositivos móveis. COMPRASNET: UNIDADE = LICENÇA	5000	Licença
8	Fornecimento de licenças de uso de solução de Filtro de Conteúdo. COMPRASNET: UNIDADE = LICENÇA	5000	Licença
9	Solução de Segurança de Perímetro de Rede Grande porte	4	Unidade
10	Solução de Segurança de Perímetro de Rede Médio Porte	4	Unidade
11	Solução de Segurança de Perímetro de Rede Pequeno Porte	4	Unidade
12	Fornecimento de licenças de uso de solução de AntiSpam para Correio Eletrônico Gateway de E-Mail. COMPRASNET: UNIDADE = LICENÇA	5000	Licença
13	Treinamento por item	150	Horas

Obs: Havendo divergências entre as especificações deste anexo e as do sistema, prevalecerão as deste anexo.

4.1. Especificação Detalhada:

1.1.1. Os detalhamentos das especificações dos itens constam no Anexo A deste Termo - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE SEGURANÇA DE TI.

5. DOS RECURSOS ORÇAMENTÁRIOS

5.1. As despesas decorrentes da Ata de Registro de Preços correrão pela fonte de recursos da CONTRATANTE, a ser informada quando da lavratura do instrumento contratual.

6. DA EXECUÇÃO E DO RECEBIMENTO

6.1. Quanto à execução:

6.1.1. O objeto contratual deverá ser executado em conformidade com as especificações estabelecidas neste instrumento, em um prazo máximo de 90 (noventa) dias úteis contado a partir do recebimento da ordem de serviço ou instrumento hábil.

6.1.2. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de execução, e aceitos pela CONTRATANTE, não serão considerados como inadimplemento contratual.

6.2. Quanto ao recebimento:

6.2.1. PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela CONTRATANTE.

6.2.2. DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após a verificação da qualidade e quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

7. DO PAGAMENTO

7.1. O pagamento advindo do objeto da Ata de Registro de Preços será proveniente dos recursos da ETICE e será efetuado mensalmente até 30 (trinta) dias a contar da data da apresentação da Nota Fiscal/Fatura devidamente atestada pelo gestor da contratação, mediante crédito em conta corrente em nome da contratada, exclusivamente no Banco Bradesco S/A, conforme Lei nº 15.241, de 06 de dezembro de 2012.

7.1.1. A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

7.2. Não será efetuado qualquer pagamento à CONTRATADA, em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

7.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento.

7.4. No caso de atraso de pagamento, desde que a contratada não tenha concorrido de alguma forma para tanto, serão devidos pela contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

7.4.1. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos, N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento, I = Índice de compensação financeira = 0,00016438 e VP = Valor da prestação em atraso.

7.5. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:

7.5.1. Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União, Certidão Negativa de Débitos Estaduais, Certidão Negativa de Débitos Municipais, Certificado de Regularidade do FGTS - CRF, Certidão Negativa de Débitos Trabalhistas – CNDT.

7.6. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, autenticada por cartório competente ou por servidor da Administração, ou publicação em órgão da imprensa oficial. Caso a documentação tenha sido emitida pela internet, só será aceita após a confirmação de sua autenticidade.

8. DAS SANÇÕES ADMINISTRATIVAS

8.1. Pela inexecução total ou parcial do contrato, a contratante poderá, garantida a prévia defesa, aplicar a contratada, nos termos do art. 83 da Lei nº 13.303/2016, as seguintes penalidades:

8.1.1. Advertência

8.1.2. Multas, estipuladas na forma a seguir:

a) Multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento) pela inobservância do prazo fixado para apresentação da garantia.

b) Multa diária de 0,3% (três décimos por cento), no caso de atraso na execução do objeto contratual até o 30º (trigésimo) dia, sobre o valor da nota de empenho ou instrumento equivalente e rescisão contratual, exceto se houver justificado interesse público em manter a avença, hipótese em que será aplicada apenas a multa.

c) Multa diária de 0,5% (cinco décimos por cento), no caso de atraso na execução do objeto contratual superior a 30 (trinta) dias, sobre o valor da nota de empenho ou instrumento equivalente. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior.

d) Multa de 0,1% (um décimo por cento), sobre o valor da nota de empenho ou instrumento equivalente, em caso de descumprimento das demais cláusulas contratuais, elevada para 0,3% (três décimos por cento), em caso de reincidência.

e) Multa de 20% (vinte por cento), sobre o valor do contrato, no caso de desistência da execução do objeto ou rescisão contratual não motivada pela contratante.

8.2. Suspensão temporária de participação em licitação e impedimento de contratar com a entidade sancionadora, por prazo não superior a 2 (dois) anos.

9. DAS OBRIGAÇÕES DA CONTRATADA

9.1. Executar o objeto em conformidade com as condições deste instrumento.

9.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

9.3. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

9.4. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

9.5. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

9.6. Refazer, substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo fixado pelo (s)

órgão (s) /entidade (s) participante (s) do SRP (Sistema de Registro de Preços), contado da sua notificação.

9.7. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

9.8. Providenciar a substituição de qualquer empregado que esteja a serviço da contratante, cuja conduta seja considerada indesejável pela fiscalização da contratante.

9.9. Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, **e demais normas do Ministério do Trabalho, relativos a segurança e a medicina do trabalho**, bem como a Legislação correlata em vigor a ser exigida.

9.10. Disponibilizar nos termos da Lei nº 15.854, de 24/09/2015, vagas de empregos a presos em regime semiaberto, aberto, em livramento condicional e egressos do sistema prisional e aos jovens do sistema socioeducativo entre 16 e 18 anos, que estejam cumprindo medida de semiliberdade. Caso a execução contratual não necessite, ou necessite de 5 (cinco) ou menos trabalhadores, a reserva de vagas será facultativa.

9.11. Encaminhar mensalmente, respectivamente, à CISPE/SAP e à SPS, a folha de frequência dos presos e egressos e/ou jovens do sistema socioeducativo, contemplados com a reserva de vagas. Caso a contratação não esteja obrigada a disponibilizar vagas nos termos da Lei nº 15.854, de 24/09/2015 ficará dispensada do envio da folha de frequência.

9.12. Fornecer os equipamentos novos e de primeiro uso e os softwares deverão está em suas últimas versões e com atualização sem custo no período de garantia.

10. DAS OBRIGAÇÕES DA CONTRATANTE

10.1. Solicitar a execução do objeto à contratada através da emissão de Ordem de Fornecimento/ Serviço.

10.2. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal nº 13.303/2016.

10.3. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

10.4. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

10.5. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.

10.6. Aplicar as penalidades previstas em lei e neste instrumento.

11. DA FISCALIZAÇÃO

11.1. A execução contratual será acompanhada e fiscalizada por um gestor especialmente designado para este fim pela contratante, a ser informado quando da lavratura do instrumento contratual.

12. PRAZO DE VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

12.1. A Ata de Registro de Preços terá validade pelo prazo de 12 (doze) meses, contados a partir da data da sua publicação.

13. DA GERÊNCIA DA ATA DE REGISTRO DE PREÇOS

13.1. Caberá à Empresa de Tecnologia da Informação do Ceará - ETICE o gerenciamento da Ata de Registro de Preços, no seu aspecto operacional e nas questões legais, em conformidade com as normas do Decreto Estadual nº 32.824/2018, publicado no DOE de 11/10/2018.

14. PRAZO DE VIGÊNCIA E DE EXECUÇÃO DO CONTRATO

14.1. Os prazos de vigência e de execução contratual serão de 24 (vinte e quatro) meses, a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016.

14.2. Os prazos de vigência e de execução poderão ser prorrogados nos termos do que dispõe o art. 71 e 81 da Lei Federal nº 13.303/2016.

14.3. A publicação resumida deste contrato dar-se-á nos termos do § 2º do art. 51 da Lei nº 13.303/2016.

15. DOS ANEXOS DO TERMO DE REFERÊNCIA

ANEXO A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE SEGURANÇA DE TI
ANEXO B - ACORDO DE NÍVEL DE SERVIÇO
ANEXO C - ÓRGÃO PARTICIPANTE
ANEXO D – MODELO DE GESTÃO DO CONTRATO

Responsável pela elaboração do Termo de Referência:

_____

Álvaro Claudio Maia
Diretor de Tecnologia e Inovação - DITEC

ANEXO A - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE SEGURANÇA DE TI

	Item	Descrição	Qtde	Unidade de Medida
Grupo1	1	Fornecimento de licenças de uso de solução corporativa de antivírus, anti-exploit/anti-ransomware para estações de trabalho com gerência em nuvem.	5000	Licença
	2	Fornecimento de licenças de uso de solução corporativa de antivírus de anti-exploit/anti-ransomware para servidores com gerência em nuvem.	500	Licença
	3	Fornecimento de licenças de criptografia de arquivos de rede	5000	Licença
	4	Fornecimento de licenças de criptografia de discos	5000	Licença
	5	Fornecimento de licenças de criptografia para mídias removíveis	5000	Licença
	6	Fornecimento de licenças de criptografia de dados na nuvem	5000	Licença
	7	Fornecimento de licenças de uso de solução de controle de dispositivos móveis	5000	Licença
	8	Fornecimento de licenças de uso de solução de Filtro de Conteúdo	5000	Licença
	9	Solução de Segurança de Perímetro de Rede Grande porte	4	Unidade
	10	Solução de Segurança de Perímetro de Rede Médio Porte	4	Unidade
	11	Solução de Segurança de Perímetro de Rede Pequeno Porte	4	Unidade
	12	Fornecimento de licenças de uso de solução de AntiSpam para Correio Eletrônico Gateway de E-Mail	5000	Licença
	13	Treinamento por item	150	Horas

1. CARACTERÍSTICAS GERAIS - ITENS 1 e 2

1.1. Todos os componentes que fazem parte da solução, de segurança para servidores, estações de trabalho deverão ser fornecidas por um único fabricante.

1.2. O console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a fermentas para a monitoração e controle da proteção dos dispositivos;

1.3. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

1.4. Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

1.5. Deve possuir capacidade de realizar a integração com soluções de firewalls para criar políticas automáticas em caso de ataques em massa nos computadores e servidores;

1.6. A console deve permitir a divisão dos computadores, dentro da estrutura de gerenciamento em grupos;

1.7. Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção.

1.8. Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários;
1.9. A instalação deve ser feita via cliente específico por download da gerência central ou também via email de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;
1.10. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;
1.11. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
1.12. Deve permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política.
1.13. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;
1.14. Atualização incremental, remota e em tempo real, da vacina dos Antivírus e do mecanismo de verificação (Engine) dos clientes;
1.15. Permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;
1.16. Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;
1.17. Utilizar protocolos seguros padrão HTTPS para comunicação entre console de gerenciamento e clientes gerenciados.
1.18. As mensagens geradas pelo agente deverão estar no idioma em Português ou permitir a sua edição.
1.19. Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;
1.20. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;
1.21. Possibilidade de exibir informações como nome da máquina, versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;
1.22. Capacidade de geração de relatórios, estatísticos ou gráficos, tais como:
1.22.1. Detalhar quais usuários estão ativos, inativos ou desprotegidos, bem como detalhes dos mesmos;
1.22.2. Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, bem como detalhes das varreduras e dos alertas nos computadores;
1.22.3. Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;
1.22.4. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;
1.22.5. Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;
1.22.6. Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;
1.22.7. Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.
1.23. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;

1.24. Deve fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais. Deve ser bloqueado o upload ou removida a informação confidencial antes do envio do arquivo;
1.25. As portas de comunicação deverão ser configuráveis. A comunicação deverá permitir QoS para controlar a largura de banda de rede.
1.26. A solução deverá permitir a seleção da versão do software de preferência, permitindo assim o teste da atualização sobre um grupo de PCs piloto antes de implantá-lo para toda a rede. Permitir ainda selecionar um grupo de computadores para aplicar a atualização para controlar a largura de banda de rede. A atualização da versão deverá ser transparente para os usuários finais.
1.27. O agente antivírus deverá proteger laptops, desktops e servidores em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deve fornecer controle de dispositivos terceiros e, controle de acesso à web;
1.28. Deve possuir mecanismo contra a desinstalação do endpoint pelo usuário e cada dispositivo deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os dispositivos;
1.29. Deve prover no endpoint a solução de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente;
1.30. Deve prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits;
1.31. Deve permitir a monitoração e o controle de dispositivos removíveis nos equipamentos dos usuários, como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;
1.32. O controle de dispositivos deve ser ao nível de permissão, somente leitura ou bloqueio;
1.33. Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis seguras, CD, DVD, Blu-ray, floppy drives, interfaces de rede sem fio, modems, bluetooth, infravermelho, MTP (Media Transfer Protocol) tais como Blackberry, iPhone e Android smartphone e PTP (Picture Transfer Protocol) como câmeras digitais;
1.34. A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para estações de trabalho e servidores e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores;
1.35. Deverá possuir interface gráfica web, com suporte a língua portuguesa (padrão brasileiro);
1.36. A Console de administração deve incluir um painel com um resumo visual em tempo real para verificação do status de segurança;
1.37. Deverá fornecer filtros pré-construídos que permitam visualizar e corrigir apenas os computadores que precisam de atenção;
1.38. Deverá exibir os PCs gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc), e classificar os PCs em conformidade;
1.39. Uma vez que um problema seja identificado, deverá permitir corrigir os problemas remotamente, com no mínimo as opções abaixo:
1.39.1. Proteger o dispositivo com a opção de início de uma varredura;

1.39.2. Forçar uma atualização naquele momento;
1.39.3. Ver os detalhes dos eventos ocorridos;
1.39.4. Executar verificação completa do sistema;
1.39.5. Forçar o cumprimento de uma nova política de segurança;
1.39.6. Mover o computador para outro grupo;
1.39.7. Apagar o computador da lista;
1.40. Atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;
1.41. Gravar um log de auditoria seguro, que monitore a atividade na console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;
1.42. Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;
1.43. Deve conter vários relatórios para análise e controle dos usuários e endpoints. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;
1.44. Fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:
1.44.1. Nome do dispositivo;
1.44.2. Início da proteção;
1.44.3. Ultimo usuário logado no dispositivo;
1.44.4. Último update;
1.44.5. Último escaneamento realizado;
1.44.6. Status de proteção do dispositivo;
Grupo a qual o dispositivo faz parte;
1.45. Permitir a execução manual de todos estes relatórios danos formatos CSV e PDF;

2. SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO - ITEM 1

2.1. Características básicas do agente de proteção contra malwares:

2.1.1. Pré-execução do agente para verificar o comportamento malicioso e detectar malware desconhecido;
2.1.2. O agente deve buscar algum sinal de malware ativo e detectar malwares desconhecidos;
2.1.3. O agente deve ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para detectar a presença de ameaças;
2.1.4. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
2.1.5. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
2.1.6. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;
2.1.7. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
2.1.8. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
2.1.9. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

2.1.10. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
2.1.11. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);
2.1.12. Suportar máquinas com arquitetura 32-bit e 64-bit;
2.1.13. O cliente para instalação em estações de trabalho deverá ser compatível com os sistemas operacionais, Mac OS X 10.10, 10.11, 10.12, Microsoft Windows 7, 8 e 10;
2.1.14. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
2.1.15. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;

2.2. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS):

2.2.1. Deverá possui atualização periódica de novas assinaturas de ataque;
2.2.2. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo.
2.2.3. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
2.2.4. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
2.2.5. Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.
2.2.6. Deve possuir técnicas de proteção, que inclui:
2.2.6.1.1. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;
2.2.6.1.2. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;
2.2.6.1.3. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
2.2.6.1.4. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);
2.2.6.1.5. Verificação de ameaças web avançadas: bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

2.3. Funcionalidade de Antivírus e AntiSpyware:

2.3.1. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

2.3.2. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.
2.3.3. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;
2.3.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (white-lists) para que não sejam verificados pelo produto;
2.3.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;
2.3.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;
2.3.7. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
2.3.8. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;
2.3.9. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;
2.3.10. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
2.3.11. Antivírus de Web (verificação de sites e downloads contra vírus);
2.3.12. Controle de acesso a sites por categoria;
2.3.13. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, ou seja, sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.
2.3.14. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;
2.3.15. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;
2.3.16. Capacidade de verificar somente arquivos novos e alterados;
2.3.17. Funcionalidade antirroubo de credencial;
2.3.18. Funcionalidade antielevação de privilégio;
2.3.19. Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

2.4. Funcionalidade de detecção Proativa de reconhecimento de novas ameaças:

2.4.1. Funcionalidade de detecção de ameaças via técnicas de deep machine learning;
2.4.2. Funcionalidade de detecção de ameaças desconhecidas que estão em memória;

2.4.3. Capacidade de detecção, e bloqueio proativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);
2.4.4. Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;
2.4.5. Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

2.5. Funcionalidade de proteção contra ransomwares:

2.5.1. Para estações de trabalho, dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
2.5.2. Dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;
2.5.3. A solução deverá prevenir ameaças e interromper que elas sejam executadas em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas.
2.5.4. Deve possuir uma tecnologia anti-exploit baseada em comportamento, reconhecendo e bloqueando as mais comuns técnicas de exploração de vulnerabilidade, protegendo os endpoints de ameaças desconhecidas e vulnerabilidades zero-day.
2.5.5. Deve ser realizada a detecção e o bloqueio de, pelo menos, as seguintes técnicas de exploit:
2.5.5.1. DEP (Data Execution Prevention);
2.5.5.2. Address Space Layout Randomization (ASLR);
2.5.5.3.Bottom Up ASLR;
2.5.5.4. Null Page;
2.5.5.5.Anti-HeapSpraying;
2.5.5.6.Dynamic Heap Spray;
2.5.5.7.Import Address Table Filtering (IAF);
2.5.5.8.VTable Hijacking;
2.5.5.9.Stack Pivot and Stack Exec;
2.5.5.10.SEHOP;
2.5.5.11.Stack-based ROP (Return-Oriented Programming);
2.5.5.12.Control-Flow Integrity (CFI);
2.5.5.13.Syscall;
2.5.5.14.WOW64;
2.5.5.15.Load Library;
2.5.5.16.Shellcode;
2.5.5.17.VBScript God Mode;
2.5.5.18.Application Lockdown;
2.5.5.19.Process Protection;
2.5.5.20.Network Lockdown.

2.5.6. A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal. Deste modo a solução deve ser capaz de fazer a limpeza e remoção completa do ransomware na máquina do usuário.
2.5.7. Deve fornecer também uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações

feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados.
2.5.8. A console de monitoração e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas as ferramentas para a monitoração e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware.
2.5.9. A console deverá apresentar *Dashboard* com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints.

2.6. Solução de endpoint detection and response (EDR)

2.6.1. A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;
2.6.2. Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.
2.6.3. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.
2.6.4. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:
2.6.4.1.Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;
2.6.4.2.Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;
2.6.4.3.Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;
2.6.4.4.Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;
2.6.5. A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
2.6.6. O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;
2.6.7. Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
2.6.8. Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
2.6.9. Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;
2.6.10. Deve ser capaz de exibir todos os processos, acessos, arquivos escritos, arquivos lidos e chaves de registros gerados pela ameaça.
2.6.11. Deve ser capaz de exibir linha de comando gerada pelo processo suspeito.

2.7. Funcionalidade de Controle de aplicações e dispositivos:

2.7.1. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
2.7.2. Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;

2.7.3. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
2.7.4. Oferecer proteção para chaves de registro e controle de processos;
2.7.5. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome e no Hash do arquivo;
2.7.6. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
2.7.7. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
2.7.8. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
2.7.9. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
2.7.10. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
2.7.11. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
2.7.12. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
2.7.13. A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;
2.7.14. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:
2.7.14.1.Permitir que todos os dispositivos do mesmo modelo;
2.7.14.2.Permitir que um único dispositivo com base em seu número de identificação único;
2.7.14.3.Permitir o acesso total;
2.7.14.4.Permitir acesso somente leitura;
2.7.15. Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

2.8. Funcionalidade de Proteção e Prevenção a Perda de Dados

2.8.1. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;
2.8.2. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);
2.8.3. Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;
2.8.4. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:
2.8.4.1.Números de cartões de crédito;
2.8.4.2.Números de contas bancárias;
2.8.4.3.Números de Passaportes;
2.8.4.4.Endereços;
2.8.4.5.Números de telefone;
2.8.4.6.Códigos postais definidas por países como França, Inglaterra, Alemanha, EUA, etc;
2.8.4.7.Lista de e-mails;

2.8.5. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;
2.8.6. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.
2.8.7. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;
2.8.8. Permitir o controle de dados para no mínimo os seguintes meios:
2.8.8.1.Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);
2.8.8.2.Anexado no navegador (ao menos IE, Firefox e Chrome);
2.8.8.3.Anexado no cliente de mensagens instantâneas (ao menos Skype);
2.8.8.4.Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

3. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA SERVIDORES – ITEM 2

3.1. Características básicas do agente de proteção contra malwares:

3.1.1. A solução deverá ser capaz de proteger servidores contra malwares, arquivos e tráfego de rede malicioso, controle de periféricos, controle de acesso à web, controle de aplicativos em um único agente instalado nos servidores;
3.1.2. Deve realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;
3.1.3. O agente host deve buscar algum sinal de malwares ativos e detectar malwares desconhecidos;
3.1.4. O agente deve realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
3.1.5. A solução deve manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
3.1.6. Deve realizar a verificação de todos os arquivos acessados em tempo real, mesmo durante o processo de boot;
3.1.7. Deve realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
3.1.8. Deve realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
3.1.9. Deve proteger os navegadores Internet Explorer, Firefox, Chrome, Opera e Safari, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;
3.1.10. Deve permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
3.1.11. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);
3.1.12. O cliente para instalação em estações de trabalho devera ser compatível com os sistemas operacionais abaixo:
3.1.12.1.Windows Server 2016;

3.1.12.2.Windows Server 2012 R2 (64 bit);
3.1.12.3.Windows Server 2012 (64 bit);
3.1.12.4.Windows Server 2008 R2 (64 bit);
3.1.12.5.Windows Server 2008 (32 or 64 bit);
3.1.12.6.Amazon Linux;
3.1.12.7.CentOS;
3.1.12.8.Novell Open Enterprise Server 2015 SP1;
3.1.12.9.Oracle Linux 6.2/7;
3.1.12.10.Red Hat Enterprise Linux 6/7;
3.1.12.11.SUSE 11/12;
3.1.12.12.Ubuntu Server 14.04/16.04;
3.1.13. Deve suportar o uso de servidores usados para atualização em cache para diminuir a largura de banda usada nas atualizações;
3.1.14. Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;
3.1.15. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
3.1.16. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção;
3.1.17. Possuir funcionalidade de Applocker que permite criar uma lista de aplicações que poderam ser executadas no servidor. Todos as aplicações não listadas devem ser bloqueadas sua execução.

3.2. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as funcionalidades:

3.2.1. Possuir proteção contra exploração de buffer overflow;
3.2.2. Possuir proteção contra-ataques de Negação de Serviço (Denial of Service - DoS), Port-Scan, MAC Spoofing e IP Spoofing;
3.2.3. Deverá possui atualização periódica de novas assinaturas de ataque;
3.2.4. Capacidade de reconhecer e bloquear automaticamente as aplicações em clientes baseando-se na impressão digital (hash) do arquivo.
3.2.5. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
3.2.6. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados.
3.2.7. Ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow.
3.2.8. Deve possuir técnicas de proteção, que inclui:
3.2.8.1.Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;
3.2.8.2.Algoritmo correspondente **padrão** - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;
3.2.8.3.Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

3.2.8.4.Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);
3.2.8.5.Verificação de ameaças web avançadas**:** bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados;

3.3. Funcionalidade de Antivírus e AntiSpyware:

3.3.1. Proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos.

3.3.2. Proteção anti-malware deverá ser nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante.

3.3.3. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;

3.3.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;

3.3.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real nos servidores;

3.3.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;

3.3.7. Capacidade de detectar arquivos através da reputação dos mesmos;

3.3.8. Capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;

3.3.9. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;

3.3.10. Capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;

3.3.11. Deverá detectar tráfego de rede para comandar e controlar os servidores;

3.3.12. Proteger arquivos de documento contra-ataque do tipo ransomwares;

3.3.13. Proteger que o ataque de ransomware seja executado remotamente;

3.3.14. Permitir o envio de amostras de malwares para a nuvem de inteligência do fabricante;

3.3.15. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;

3.3.16. Antivírus de Web (verificação de sites e downloads contra vírus);

3.3.17. Controle de acesso a sites por categoria;

3.3.18. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox, Safari, Opera e Chrome), fornecendo controle da Internet independentemente do browser utilizado sem utilizar um plugin, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites.

3.3.19. O Controle da Web deve controlar o acesso a sites impróprios, com no mínimo 14 categorias de sites inadequados. Deve ainda permitir a criação de lista branca de sites sempre permitidos e lista negra de sites que devem ser bloqueados sempre;

3.3.20. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas para a console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;

3.3.21. Capacidade de verificar somente arquivos novos e alterados;
3.3.22. Funcionalidade antirroubo de credencial;
3.3.23. Funcionalidade antielevação de privilégio;
3.3.24. Funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.
3.3.25. Capacidade de habilitar mensagens de desktop para a Proteção contra Ameaças;
3.3.26. Capacidade de adicionar exclusão de varredura para arquivos, pastas, processos, sites, aplicativos e tipos de explorações detectadas;

3.4. Funcionalidade de detecção Pró-Ativa de reconhecimento de novas ameaças:

3.4.1. Funcionalidade de detecção de ameaças via técnicas de deep machine learning;
3.4.2. Funcionalidade de detecção de ameaças desconhecidas que estão em memória;
3.4.3. Capacidade de detecção, e bloqueio pró-ativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);
3.4.4. Capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;
3.4.5. Capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada

3.5. Funcionalidade de proteção contra ransomwares:

3.5.1. Deve dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
3.5.2. Deve dispor de capacidade de remediação da ação de criptografia maliciosa dos ransomwares;
3.5.3. Deve dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;

3.6. Solução de endpoint detection and response (EDR)

3.6.1. A solução deve ter capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;
3.6.2. Deve ter a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante.
3.6.3. Em caso de incidente a solução deve mostrar a trilha da infecção de forma visual, mostrando o início, todas as interações do malware e o ponto final de bloqueio.
3.6.4. Após a análise da nuvem de inteligência do fabricante a solução deve apresentar um relatório sobre a ameaça contendo no mínimo:
3.6.4.1.Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;
3.6.4.2.Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento como o Vírus Total;

3.6.4.3.Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;
3.6.4.5.Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, informações de certificado;
3.6.5. A solução de EDR deverá ser integrado ao agente de antivírus a ser instalado com um com agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
3.6.6. O gerenciamento da solução de EDR deverá ser feito a partir da mesma console de gerenciamento da solução antivírus;
3.6.7. Deve fornecer guias de repostas a incidentes, fornecendo visibilidade sobre o escopo de um ataque, como ele começou, o que foi impactado, e como responder;
3.6.8. Deve ser capaz de responder ao incidente com opção de isolamento da máquina, bloqueio e limpeza da ameaça;
3.6.9. Deve ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;
3.6.10. Deve ser capaz de exibir todos os processos, acessos, arquivos escritos, arquivos lidos e chaves de registros gerados pela ameaça.
3.6.11. Deve ser capaz de exibir linha de comando gerada pelo processo suspeito

3.7. Funcionalidade de Controle de aplicações e dispositivos:

3.7.1. Possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
3.7.2. Atualiza automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;
3.7.3. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
3.7.4. Oferecer proteção para chaves de registro e controle de processos;
3.7.5. Proibir através de política a inicialização de um processo ou aplicativo baseado em nome e no Hash do arquivo;
3.7.6. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
3.7.7. Deve possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
3.7.8. Gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB). Permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
3.7.9. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
3.7.10. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
3.7.11. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
3.7.12. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
3.7.13. A gestão desses dispositivos deverá feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;
3.7.14. Permitir a autorização de um dispositivo com no mínimo as seguintes opções:

3.7.14.1.Permitir que todos os dispositivos do mesmo modelo;
3.7.14.2.Permitir que um único dispositivo com base em seu número de identificação único;
3.7.14.3.Permitir o acesso total;
3.7.14.4.Permitir acesso somente leitura;
3.7.15. Permitir ainda o bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

3.8. Funcionalidade de Proteção e Prevenção a Perda de Dados

3.8.1. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;
3.8.2. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);
3.8.3. Possibilitar o bloqueio, somente registrar o evento na Console de administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;
3.8.4. Deve possuir listas de CCLs pré-configurados com no mínimo as seguintes identificações:
3.8.4.1.Números de cartões de crédito;
3.8.4.2.Números de contas bancárias;
3.8.4.3.Números de Passaportes;
3.8.4.4.Endereços;
3.8.4.5.Números de telefone;
3.8.4.6.Códigos postais definidas por países como França, Inglaterra, Alemanha, EUA, etc;
3.8.4.7.Lista de e-mails;
3.8.5. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;
3.8.6. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo.
3.8.7. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;
3.8.8. Permitir o controle de dados para no mínimo os seguintes meios:
3.8.8.1.Anexado no cliente de e-mail (ao menos Outlook e Outlook Express);
3.8.8.2.Anexado no navegador (ao menos IE, Firefox e Chrome);
3.8.8.3.Anexado no cliente de mensagens instantâneas (ao menos Skype);
3.8.8.4.Anexado a dispositivos de armazenamento (ao menos USB, CD/DVD);

4. CARACTERÍSTICAS GERAIS DE CRIPTOGRAFIA - ITEM 3,4 e 5

4.1. Console de Gerenciamento:

4.1.1. O console administrativa da ferramenta irá gerir as chaves de criptografia centralmente e permitir a administração de políticas e dispositivos protegidos.
4.1.2. A console permite também o gerenciamento de múltiplos sistemas operacionais (Windows e Mac) e sistemas de criptografia Microsoft BitLocker (caso necessário).

4.1.3. Através da console é possível gerar relatórios de uso da ferramenta, assim como a auditoria do status de criptografia de todos os dispositivos e de quem tem acesso aos mesmos.
4.1.4. É possível definir usuários administrativos com perfis específicos de acesso e permissão sobre as configurações e políticas da ferramenta.
4.1.5. Todos os dispositivos, regras e usuários da ferramenta devem ser gerenciados pela console de forma central e integrada aos sistemas de usuários (Active Directory) já existentes no CLIENTE.

4.2. Módulo de Criptografia de Arquivos em Rede (File Share)

4.2.1. Deve proteger arquivos e pastas armazenados localmente ou em rede. Os arquivos também devem estar protegidos se estiverem em trânsito.
4.2.2. Deve permitir que somente usuários que tenham a(s) chave(s) de criptografia acessem o conteúdo do(s) arquivo(s).
4.2.3. Deve oferecer criptografia inteligente e transparente para o usuário final.
4.2.4. A definição de regras e políticas para cada usuário ou grupo de usuários devem ser possíveis e controladas centralmente através da console do produto.
4.2.5. Deve oferecer proteção efetiva contra vazamento de dados através de qualquer mídia ou tecnologia de envio de arquivos, mensagens ou cópia não autorizada.

4.3. Módulo de Criptografia de Discos (Device Encryption):

4.3.1. O módulo de criptografia de discos permite a criptografia total do disco e protege todos os dados contra perda e roubo.
4.3.2. O módulo deve apresentar uma rápida criptografia inicial, com baixo impacto na performance.
4.3.3. A solução deve ter certificação FIPS 140-2 e CC EAL-4 .
4.3.4. A solução deve permitir duplo fator de autenticação, Single-Sign-on e Power authorization (POA).
4.3.5. A solução também deve permitir recuperação de senha através do help-desk da empresa ou de um sistema de recuperação de senhas ativado pelo próprio usuário.

4.4. Módulo de Criptografia para mídias removíveis (Data Exchange)

4.4.1. O módulo de criptografia de mídias removíveis deve proteger dados armazenados em pen-drives, cartões de memória e HDs externos.
4.4.2. Deve ser possível compartilhar dados de forma segura com o mínimo impacto ao usuário final.
4.4.3. Deve permitir que usuários utilizem dispositivos e mídias removíveis garantindo a segurança dos dados corporativos de forma transparente usando chaves e políticas.
4.4.4. Deve impor regras de criptografia de arquivos copiados para dispositivos móveis por política e controle de acesso.
4.4.5. Deve permitir seleção de dispositivos que podem e não podem ser utilizados pelos usuários. (whitelist - blacklist)
4.4.6. Deve ser possível ter arquivos criptografados e não criptografados na mesma mídia removível.
4.4.7. Deve ser possível proteger dados em midias removiveis contra perda, manter o controle de acesso e proteger outras mídias de armazenamento como CD/DVD, memory cards, entre outros.

4.5. Módulo de Criptografia de Dados na Nuvem (Encryption for Cloud Storage)

4.5.1. Deve adicionar segurança por criptografia em documentos armazenados em nuvem.

4.5.2. O módulo deve aplicar criptografa em pastas na nuvem de forma transparente para o usuário final.
4.5.3. Deve ser possível o controle de políticas de criptografia e chaves e que as mesmas permaneçam nas premissas do CLIENTE.
4.5.4. Deve oferecer suporte aos principais fornecedores de armazenamento em nuvem: Dropbox, GoogleDrive, Egnyte, Onedrive, entre outros.
4.5.5. Deve oferecer suporte a nuvens privadas e públicas, assim como nuvens híbridas.
4.5.6. Deve proteger os arquivos assim que eles são enviados da organização para a nuvem.
4.5.7. Fortalecer políticas de segurança de dados e a confidencialidade dos dados sigilosos do CLIENTE.
4.5.8. Permitir o compatilhamento de arquivos dentro e fora da empresa e entre dispositivos (PC, Smartphones, Tablets, entre outros).
4.5.9. E deve permitir o acesso a dados criptografados através de smartphones e tables, utilizando aplicativo gratuito desenvolvido pelo fabricante para sistema iOS e Android.

5. DESCRIÇÃO DA SOLUÇÃO DE CONTROLE DE DISPOSITIVOS MÓVEIS – ITEM 7

5.1. Especificações Gerais

5.1.1. A solução deve ser realizar o gerenciamento de dispositivos móveis, conteúdo, aplicativos e segurança;
5.1.2. Deve possuir uma console de gerenciamento intuitiva de fácil instalação, configuração e manutenção;
5.1.3. A solução deve ser capaz de gerenciar os dispositivos abaixo:
5.1.3.1.Apple iPhone com iOS 9 ou superior;
5.1.3.2.Apple iPad ou iPod Touch com iOS 9 ou superior;
5.1.3.3.Android 4.4 ou superior;
5.1.3.4.Windows Phone 8.1;
5.1.3.5.Windows 10 Mobile ou Mobile Enterprise;
5.1.3.6.Windows 10 Pro, Enterprise, Education ou Home;
5.1.4. Deve realizar a inclusão dos dispositivos móveis no console de gerenciamento através de:
5.1.4.1.Utilizando assistente de inscrição do dispositivo;
5.1.4.2.Inscrição do dispositivo através de envio de email de instruções;
5.1.4.3.Inserção do dispositivo através de portal de autoatendimento;
5.1.4.4.Inserção do dispositivo no console de gerenciamento;
5.1.4.5.Inserção através do Android Zero-Touch;
5.1.4.6.Inserção através do Apple configurator;
5.1.4.7.Instalação via arquivo *.ppkg;
5.1.4.8.Instalação via lojas de aplicativos como Apple Play Store ou Google Play Store;
5.1.5. Deve permitir a definição dos pacotes padrões para dispositivos corporativos e pessoais;
5.1.6. Deve implementar a atribuição automática das políticas baseadas em grupos;
5.1.7. A plataforma deve oferecer proteção de segurança para os dispositivos móveis;
5.1.7.1. Deve prover análise dos aplicativos no momento da instalação em busca de malwares utilizando técnicas de machine learning;
5.1.7.2.Deve verificar os aplicativos instalados anteriormente nos dispositivos em busca de malwares;
5.1.7.3.Deve permitir realizar a análise dos aplicativos sob demanda ou em intervalos definidos;
5.1.7.4.Deve possuir proteção contra aplicativos maliciosos, sites maliciosos, aplicativos de baixa reputação, adware e outros aplicativos possivelmente indesejados (PUAs);
5.1.7.5.Deve se integrar a nuvem de inteligência do fabricante para identificar novas ameaças;

5.1.7.6.Deve possuir conexão criptografada entre o dispositivo e a console de gerenciamento;
5.1.7.7.Deve possui controle sobre o acesso ao email corporativo pelo dispositivo, baseado em conformidade;
5.1.7.8.Deve possuir métodos de segundo fator de autenticação para aceso ao email, através de senha e certificado;
5.1.7.9.Deve possuir controle de acesso a rede por conformidade, NAC control;
5.1.7.10.Deve possuir proteção de código USSD;
5.1.7.11.Deve possuir controle de acesso a sites maliciosos;
5.1.7.12.Deve possuir proteção para ataques de *man-in-the-middle* para redes WI-FI;
5.1.7.13.Deve possuir capacidade de filtragem web com pelo menos 14 categorias de sites;
5.1.7.14.Deve possuir White e Black lists para endereços IP`s, nomes de DNS e ranges de IP`s;
5.1.7.15.Deve possuir proteção para aplicativos corporativos solicitando autenticação adicional;
5.1.7.16.Deve possuir proteção contra Phishing em mensagens de texto;
5.1.7.17.Deve possuir blacklist e whitelist para aplicações;
5.1.7.18.Deve bloquear a instalação de aplicações de fontes desconhecidas;
5.1.7.19.Deve possuir controle sobre o número máximo de tentativas de desbloqueio do dispositivo, podendo formatar o dispositivo;
5.1.7.20.Deve possuir a configuração de definir quais aplicativos são mandatórios o dispositivo deve possuir instalado;
5.1.7.21.Deve possuir a capacidade de detectar jailbreak e detecção de root nos sistemas operacionais;
5.1.8. Deve possuir a capacidade de gerenciar as aplicações da seguinte forma:
5.1.8.1.Criação de uma app store corporativa;
5.1.8.2.Instalar aplicações remotamente com ou sem a interação do usuário;
5.1.8.3.Desinstalar aplicações remotamente com ou sem a interação do usuário;
5.1.8.4.Listar todas as aplicações instaladas nos dispositivos;
5.1.8.5.Deve possuir suporte ao *Apple Volume Purschasing Program* (VPP);
5.1.8.6.Permitir ou proibir a instalação de aplicações pelos usuários;
5.1.8.7.Proibir a desinstalação de aplicações pelos usuários;
5.1.8.8.Proibir a instalação de aplicações de fontes não seguras;
5.1.8.9.Configuração remota das aplicações corporativas;
5.1.8.10.Proibir a execução de determinadas aplicações;
5.1.8.11.Gerenciar e configurar aplicações Microsoft office 365;
5.1.9. Deve possuir a proteção contra perda de dados no caso de um dispositivo ser perdido ou roubado;
5.1.9.1.Deve enviar comandos de texto a partir de números de telefone pré-definidos para executar tarefas;
5.1.9.2.Realizar o bloqueio remoto ou limpeza de um dispositivo Android perdido ou roubado;
5.1.9.3.Permitir a exibição de uma mensagem para o localizador do dispositivo;
5.1.9.4.Deve permitir configurar a complexidade mínima de senhas a serem usadas no dispositivo, como por exemplo, letras maiúsculas, números e caracteres especiais;
5.1.9.5.Deve permitir a redefinição da senha do dispositivo;
5.1.9.6.Deve possuir a função de localizar o dispositivo com tecnologia de rastreamento;
5.1.9.7.Deverá o dispositivo enviar seu último local antes que a bateria acabe;
5.1.9.8.Deverá informar sobre uma alteração do SIM.
5.1.9.9.Deve permitir que as funções possam ser acionadas a partir da console de gerenciamento ou através de um Portal de autoatendimento;
5.1.9.10.A solução deve ser capaz de controlar os recursos dos dispositivos móveis como:
5.1.9.11.Deve definir o tempo de inatividade em minutos até que a senha seja necessária;
5.1.9.12.Limitar o número máximo de tentativas até que o dispositivo seja redefinido;

5.1.9.13.Controlar o comprimento mínimo da senha;
5.1.9.14.Definir o tempo de expiração da senha;
5.1.9.15.Deve possibilitar a redefinição de senha pelo administrador;
5.1.9.16.Deve permitir a ativação de criptografia de armazenamento;
5.1.9.17.Deve permitir o controle de acesso ao cartão de memória;
5.1.9.18.Permitir a ativação e desativação da criptografia de dados do dispositivo;
5.1.9.19.Bloquear Wi-Fi;
5.1.9.20.Bloquear Bluetooth;
5.1.9.21.Bloquear transferência de dados via Bluetooth;
5.1.9.22.Bloquear transferência de dados via NFC;
5.1.9.23.Bloquear conexões USB;
5.1.9.24.Bloquear câmera;
5.1.9.25.Proteção de configurações contra modificação ou remoção pelo usuário;
5.1.9.26.Permitir e proibir o uso da iTunes Store, Google Play ou Windows Store;
5.1.9.27.Permitir e proibir o uso do navegador;
5.1.9.28.Permitir e proibir conteúdo explícito;
5.1.9.29.Permitir e proibir a câmera na tela de bloqueio;
5.1.9.30.Permitir e proibir o uso de aplicativos de terceiros por e-mail;
5.1.9.31.Permitir e proibir iCloud autosync;
5.1.9.32.Permitir e proibir configuração manual de Wi-Fi;
5.1.9.33.Permitir e proibir o envio de dados de falha para a Apple, Google, Samsung ou Microsoft (telemetria);
5.1.9.34.Permitir e proibir certificados de fontes não confiáveis;
5.1.9.35.Permitir e proibir conexão automática de Wi-Fi;
5.1.9.36.Permitir e proibir fluxo de fotos compartilhadas;
5.1.9.37.Permitir e proibir Apple Wallet ;
5.1.9.38.Permitir e proibir o dispositivo em compartilhar ponto de acesso;
5.1.9.39.Permitir e proibir a funcionalidade "Abrir com ..." para compartilhar dados entre aplicativos gerenciados e não gerenciados;
5.1.9.40.Permitir e proibir leitor de impressão digital (Touch ID) para desbloquear o dispositivo;
5.1.9.41.Permitir e proibir modificação de conta;
5.1.9.42.Permitir e proibir a modificação do uso de dados da rede celular por aplicativo;
5.1.9.43.Permitir e proibir o Centro de Controle na tela de bloqueio;
5.1.9.44.Permitir e proibir o Centro de Notificação na tela de bloqueio;
5.1.9.45.Permitir e proibir o emparelhamento de host;
5.1.9.46.Permitir e proibir autenticação de varredura da íris;
5.1.9.47.Permitir e proibir a loja do iBooks;
5.1.9.48.Permitir e proibir conteúdo sexual explícito na loja iBooks;
5.1.9.49.Permitir e proibir iMessage;
5.1.9.50.Permitir e proibir o usuário redefinir o dispositivo;
5.1.9.51.Permitir e proibir a remoção de dispositivos do gerenciamento do MDM;
5.1.9.52.Permitir e proibir o usuário criar capturas de tela;
5.1.9.53.Filtrar o acesso a sites da Web (lista negra) ou sites da lista de permissões com marcadores;
5.1.9.54.Permitir atrasar ou bloquear atualização do sistema operacional;
5.1.9.55.Permitir e proibir preenchimento automático de senha;
5.1.9.56.Permitir e proibir o compartilhamento de senha;
5.1.10. A solução deve ser capaz de configurar os recursos dos dispositivos móveis como:
5.1.10.1.Configurações do Microsoft Exchange para email;
5.1.10.2.Configurações IMAP ou POP para email;

5.1.10.3.Configurações LDAP, CardDAV e CalDAV;
5.1.10.4.Configuração de pontos de acesso;
5.1.10.5.Configurações de proxy;
5.1.10.6.Configurações de wifi;
5.1.10.7.Configurações de VPN;
5.1.10.8.Instalar certificados rai;z
5.1.10.9.Instalar certificados de cliente;
5.1.10.10.Configurar logon único (SSO) para aplicativos de terceiros (proteção de aplicativos) e páginas da empresa;
5.1.10.11.Distribuição de marcadores (Web Clips);
5.1.10.12.Forçar a atualização do iOS em dispositivos supervisionados (e exibir atualizações pendentes do iOS);
5.1.10.13.Configurar a tela de bloqueio e a tela inicial do iOS;
5.1.10.14.Configurar dos domínios gerenciados;
5.1.10.15.Configuração de firewall;
5.1.10.16.Modo de quiosque;
5.1.10.17.Permissões de aplicativos;
5.1.10.18.Ativar o modo perdido do iOS;
5.1.10.19.Configurar contas do Google;
5.1.10.20.Integrar com o Duo Security;
5.1.10.21.Configurar dispositivos para usar impressoras AirPrint;
5.1.11. A solução deve ser capaz de criar contêiner dentro dos dispositivos moveis para prover segurança;
5.1.11.1.Os contêineres devem manter os dados confidenciais e seguros;
5.1.11.2.Deve possuir mecanismos de Geo-fencing , Time-fencing e Wi-Fi fencing;
5.1.11.3.Deve utilizar criptografia FIPS 140-2 usando AES256 para os contêineres;
5.1.11.4.Deve permitir adicionar ou remover documentos de forma segura através da console de gerenciamento;
5.1.11.5.Deve controlar o acesso ao armazenamento na nuvem, como as soluções Box, Dropbox, Egnyte, Google Drive, Microsoft OneDrive e WebDAV.
5.1.11.6.Deve possuir a distribuição de documentos de forma segura através de Workspace;
5.1.11.7.Documentos armazenados no container devem ser criptografados;
5.1.11.8.A configuração de DLP deve permitir visualização dos documentos off-line;
5.1.11.9.A configuração de DLP deve permitir cópia para a área de transferência;
5.1.11.10.A configuração de DLP deve Permitir envio por e-mail em formato criptografado;
5.1.11.11.A configuração de DLP deve permitir "abrir com" sem criptografia, incluindo o envio de e-mails não criptografados;
5.1.11.12.Possuir capacidade de visualizar e editar documentos armazenados no Workspace;
5.1.11.13.Deve possuir a capacidade de bloqueio do container em caso de o dispositivo esteja fora de compliance;
5.1.11.4.Visualizar, gerenciar e criar arquivos compactados Zip e 7z;
5.1.12. Deve possuir a configuração de fácil acesso a sites corporativos através de browser customizado;
5.1.12.1.Deve possuir a configuração de logon único simples (SSO) para sites de intranet e sites mais frequentados;
5.1.12.2.Deve controlar a navegação restrita a domínios corporativos predefinidos;
5.1.12.3.Deve possuir marcadores corporativos pré-configurados;
5.1.12.4.Deve gerenciar as senhas de uso no browser;
5.1.12.5.Deve gerenciar os certificados de cliente ou usuário para autenticação em sites corporativos;

5.1.12.6.Deve gerenciar os certificados raiz;
5.1.12.7.Deve controla no browser as funcionalidades de corte, cópia e colagem de conteúdo;
5.1.12.8.Deve permiti a ativação e desativação da opção de “salvar senha” para reduzir os riscos de segurança;
5.1.13. Deve possuir administração flexível para gerenciamento de e-mails corporativos;
5.1.13.1.Deve permitir o provisionamento do acesso aos e-mails corporativos através da console de gerenciamento;
5.1.13.2.Deve possuis proteção através de contêineres para contatos, calendários e e-mails;
5.1.13.3.Deve ser capaz de realizar a remoção imediata de e-mails corporativos quando um dispositivo for perdido, roubado ou quando um funcionário deixar a empresa;
5.1.13.4.Deve restringir o acesso ao email, dependendo da conformidade e integridade do dispositivo móvel;
5.1.14. Deve realizar proteção de privacidade dos conteúdos do dispositivo móvel;
5.1.14.1.Deve detectar aplicativos que acessam dados pessoais, como o catálogo de endereços;
5.1.14.2.Deve permite identificar facilmente aplicativos que podem envolver custos ou taxas a corporação;
5.1.15. Deve ser capaz de impedir a abertura de aplicações sem que o usuário informe a senha;
5.1.16. Deve possuir capacidade de realizar autenticação através de senha única (OTP);
5.1.16.1.Deve gerar senhas de tempo único TOTP (RFC 6238) ou baseadas em contador HOTP (RFC 4226);
5.1.16.2.Deve permitir o uso com qualquer aplicativo habilitado pelo Google Authenticator para autenticação multifator;
5.1.17. Deve possuir filtragem de spam;
5.1.17.1.Deve filtrar mensagens de texto recebidas (SMS) de acordo com as regras de segurança;
5.1.17.2.Deve colocar mensagens de textos com URLs maliciosas em quarentena;
5.1.17.3.Deve permitir o bloqueio de chamadas indesejadas de acordo com os filtros definidos, por exemplo, chamadas com ID de usuário oculto.
5.1.18. Deve possuir proteção para leitura de QR Code;
5.1.18.1.Deve confirmar que as URLs de destino estão livres de conteúdo malicioso antes de abrir;
5.1.18.2.Deve sinalizar problemas de segurança com códigos QR de configurações Wi-Fi.
5.1.18.3.Deve permitir que se adicione com segurança as assinaturas de código QR aos contatos do dispositivo.

5.2 Gerenciamento das Soluções

5.2.1 A console de gerenciamento deve ser baseada em nuvem;
5.2.2 Deve possuir a capacidade de criar sub estados de gerenciamento da console;
5.2.3 Deve permitir a gerenciar da solução a partir de uma console Web;
5.2.4 Deve possuir *dashboard* flexível, permitindo a inclusão de *widgets*;
5.2.5 Deve possui mecanismos de filtros de consultas;
5.2.6 Deve possuir a capacidade de Geração de tarefas agendadas para dispositivos ou grupos únicos;
5.2.7 Deve informar o acompanhamento detalhado de status para cada tarefa;
5.2.8 Deve possuir a capacidade de repetição de tarefas em casos de falha;
5.2.9 Deve ser possível configurar níveis de acesso dos usuários a console de gerenciamento;
5.2.10 Deve permitir que mais de um usuário se autentique ao mesmo tempo na console de gerenciamento;
5.2.11 Deve manter os dados corporativos seguros, possibilitando auditorias e gerenciando aplicativos e segurança;
5.2.12 Deve permitir a localização, bloqueio e limpeza remotamente dos dispositivos para evitar a perda de dados e garantir a conformidade;

5.2.13 Deve verificar regularmente se os dispositivos estão em conformidade com as regras corporativas e avisar os administradores e usuários sobre a não conformidade;
5.2.14 Deve controlar o acesso a recursos corporativos, como e-mail ou VPN;
5.2.15 Deve permitir a gerencia de aplicativos com sua própria loja de aplicativos corporativos;
5.2.16 Deve gerenciar a segurança móvel para proteger dispositivos Android contra malware, aplicativos suspeitos e sites mal-intencionados;
5.2.17 Deve impor a separação de dados corporativos e pessoais nos dispositivos móveis;
5.2.18 Deve permitir a limpeza remotamente dados corporativos;
5.2.19 Deve limitar a quantidade máxima de dispositivos por usuários;
5.2.20 Deve se integrar com o Active Directory ou LDAP;
5.2.21 Deve coletar as seguintes informações dos dispositivos:
5.2.21.1 Utilização da memória interna (livre / usada);
5.2.21.2 Nível de carga da bateria;
5.2.21.3 IMSI (número de identificação único) do cartão SIM;
5.2.21.4 Rede da operadora de celular usada atualmente;
5.2.21.5 Modo de roaming ativado ou desabilitado;
5.2.21.6 Versão do sistema operacional;
5.2.21.7 Lista de perfis instalados;
5.2.21.8 Lista de certificados instalados;
5.2.21.9 Malware detectado no dispositivo;
5.2.21.10 Compartilhamento remoto de tela pelo Teamviewer ou AirPlay;
5.2.22 Deve possuir controle sobre gastos sobre as operadoras de celular usados no dispositivo móvel, contendo;
5.2.22.1 Desativar dados em roaming;
5.2.22.2 Desativar voz em roaming;
5.2.22.3 Controle a sincronização durante o roaming;
5.2.22.4 Configurar configurações de APN ou Carrier;
5.2.22.5 Definir limite superior de uso de dados por dispositivo;
5.2.22.6 Compare o uso de dados com o limite;
5.2.22.7 Regras de uso de rede por aplicativo;
5.2.23 Deve permitir a criação de um portal de autoatendimento para os usuários aonde o usuário tenha a capacidade de:
5.2.23.1 Registrar um novo dispositivo;
5.2.23.2 Verificar informações de conformidade do dispositivo;
5.2.23.3 Realizar a limpeza do dispositivo;
5.2.23.4 Realizar o bloqueio do dispositivo;
5.2.23.5 Realizar a localização do dispositivo;
5.2.23.6 Remover a proteção do dispositivo;
5.2.24 Relatórios
5.2.24.1 Deve possuir relatórios de inventário dos dispositivos móveis;
5.2.24.2 Deve ser possível exportar os relatórios nos formatos XLS ou CSV;
5.2.24.3 Deve possuir relatórios de conformidade de todas as atividades do administrador da solução;
5.2.24.4 Deve possuir logs de alertas detalhados;
5.2.24.5 Deve possuir relatórios de malwares encontrados nos dispositivos;
5.2.24.6 Deve possuir relatório de violação das políticas de conformidade;
5.2.24.7 Deve possuir relatório dos aplicativos instalados nos dispositivos;
5.2.24.8 Deve possuir relatório dos certificados distribuídos aos dispositivos.

6. SOLUÇÃO DE FILTRO DE CONTEÚDO – ITEM 8

6.1. Características Gerais

6.1.1. Deve possuir no mínimo 06(seis) interfaces 10/100/1000 Base-TX;
6.1.2. Deve possuir no mínimo 01(uma) inteface USB 2.0;
6.1.3. Deve possuir no mínimo 01(uma) interface para acesso console;
6.1.4. Possuir luzes indicativas no mínimo equipamento ligado, interface de rede ligada;
6.1.5. Possuir funcionalidade de balanceamento de link de internet.

6.2. Controle e proteção web

6.2.1. Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.
6.2.2. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a checagem de páginas em HTTPS.
6.2.3. Deve de-criptografar/criptografar nos protocolos TLS 1.2 e 1.3;
6.2.4. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;
6.2.5. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, Radius, *E-directory* e base de dados local;
6.2.6. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
6.2.7. Possuir pelo menos 90 categorias de URLs;
6.2.8. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
6.2.9. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;
6.2.10.Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;
6.2.11.Suportar a criação categorias de URLs customizadas;
6.2.12.Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.
6.2.13.Permitir a customização de página de bloqueio;
6.2.14.Suportar a inclusão nos logs do produto de informações das atividades dos usuários;
6.2.15.Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.
6.2.16.Deve realizar caching do conteúdo web;
6.2.17.Deve relizar filtragem por mime-type, extensão e tipos de conteúdos ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

6.3.Controle e Proteção de Aplicações

6.3.1.Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.
6.3.2.Deve de-criptografar/criptografar nos protocolos TLS 1.2 e 1.3;
6.3.3.Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e up-date de softwares.

6.3.4.Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/ SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.
6.3.5.Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)
6.3.6.O escaneamento de micro app deverá ser habilitado via console gráfica (GUI) e via comando de linha (CLI).
6.3.7.Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.
6.3.8.Atualizar a base de assinaturas de aplicações automaticamente;
6.3.9.Reconhecer aplicações em IPv6.
6.3.10.Limitar a banda usada por aplicações (*traffic shaping*).
6.3.11.Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários.
6.3.12.Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.
6.3.13.Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

6.4.Identificação de usuários

6.4.1.Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.
6.4.2.Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).
6.4.3.Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
6.4.5.Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

6.4.6.Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.
6.4.7.Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

7.SOLUÇÃO DE SEGURANÇA DE PERÍMETRO DE REDE – ITENS 9,10 e 11

7.1.Características específicas de desempenho e hardware do firewall de próxima geração (Grande Porte): ITEM 9

7.1.1.Performance mínima de 100 Gbps de throughput para firewall.
7.1.2.Performance mínima de 20 Gbps de throughput de IPS.
7.1.3.Performance mínima de 16 Gbps de throughput para controle de AV/proxy.
7.1.4.Performance mínima de 10 Gbps de throughput de VPN.
7.1.5.Suporte a, no mínimo, 30.000.000 de conexões simultâneas.
7.1.6.Suporte a, no mínimo, 300.000 novas conexões por segundo.
7.1.7.Possuir o número irrestrito quanto ao máximo de usuários licenciados.
7.1.8.Possuir armazenamento interno de no mínimo 480 GB SSD (RAID-1) hot-swap para sistema operacional, quarentena local, logs e relatórios.
7.1.9.Possuir no mínimo 64GB de memória RAM.
7.1.10.Possuir no mínimo 8 (oito) interfaces de rede 1000Base-TX.
7.1.11.Possuir no mínimo 8 (oito) módulo de expansão de interfaces com até 64 (sessenta e quatro) interfaces de rede 1000Base-TX instaladas.
7.1.12.Possuir 1 (uma) interface do tipo console ou similar.
7.1.13.Possuir 2 (duas) fonte 100-240VAC hot-swap.

7.2.Características específicas de desempenho e hardware do firewall de próxima geração (Médio Porte): ITEM 10

7.2.1.Performance mínima de 28 Gbps de throughput para firewall.
7.2.2.Performance mínima de 5 Gbps de throughput de IPS.
7.2.3.Performance mínima de 3 Gbps de throughput para controle de AV/proxy.
7.2.4.Performance mínima de 2.5 Gbps de throughput de VPN.
7.2.5.Suporte a, no mínimo, 17.000.000 de conexões simultâneas.
7.2.6.Suporte a, no mínimo, 200.000 novas conexões por segundo.
7.2.7.Possuir o número irrestrito quanto ao máximo de usuários licenciados.
7.2.8.Possuir armazenamento interno de no mínimo 160 GB SSD (para sistema operacional, quarentena local, logs e relatórios.
7.2.9.Possuir no mínimo 12GB de memória RAM.
7.2.10.Possuir no mínimo 8 (oito) interfaces de rede 1000Base-TX.
7.2.11.Possuir no mínimo 1 (um) módulo de expansão de interfaces com até 8 (oito) interfaces de rede 1000Base-TX instaladas.
7.2.12.Possuir 1 (uma) interface do tipo console ou similar.
7.2.13.Possuir 2 (duas) fonte 100-240VAC hot-swap.

7.3.Características específicas de desempenho e hardware do firewall de próxima geração (Pequeno Porte): ITEM 11

7.3.1.Performance mínima de 8 Gbps de throughput para firewall.
7.3.2.Performance mínima de 2 Gbps de throughput de IPS.
7.3.3.Performance mínima de 1.5 Gbps de throughput para controle de AV/proxy.
7.3.4.Performance mínima de 1 Gbps de throughput de VPN.
7.3.5.Suporte a, no mínimo, 6.000.000 de conexões simultâneas.

7.3.6.Suporte a, no mínimo, 80.000 novas conexões por segundo.
7.3.7.Possuir o número irrestrito quanto ao máximo de usuários licenciados.
7.3.8.Possuir armazenamento interno de no mínimo 64 GB SSD para sistema operacional, quarentena local, logs e relatórios.
7.3.9.Possuir no mínimo 6GB de memória RAM.
7.3.10.Possuir no mínimo 6 (seis) interfaces de rede 1000Base-TX.
7.3.11.Possuir 1 (uma) interface do tipo console ou similar.
7.3.12.Possuir 1 (uma) fonte 100-240VAC externa ou interna.

7.4.Características gerais para firewalls de próxima geração:

7.4.1.A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência, monitoração e logs.
7.4.2.Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
7.4.3.As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.
7.4.4.A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
7.4.5.O software deverá ser fornecido em sua versão mais atualizada.
7.4.6.O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.
7.4.7.Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.
7.4.8.A atualização de software deverá enviar avisos de atualização automáticos.
7.4.9.O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.
7.4.10.O backup e o reestabelecimento de configuração deverá ser feito localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.
7.4.11.As notificações deverão ser realizadas via email e SNMP.
7.4.12.Suportar SNMP e Netflow.
7.4.13.O firewall deverá ser stateful, com inspeção profunda de pacotes (deep packet inspection).
7.4.14.As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.
7.4.15.As políticas de NAT deverão ser customizáveis para cada regra.
7.4.16.A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS) e bloqueio de portscan.
7.4.17.Proteção contra *anti-spoofing*.
7.4.18.Suportar IPv4 e IPv6.
7.4.19.IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.
7.4.20.Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).
7.4.21.Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.
7.4.22.O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.
7.4.23.A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;
7.4.24.A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;
7.4.25.O traffic shapping (QoS) deverá ser baseado em rede ou usuário.
7.4.26.A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.
7.4.27.Deve possuir otimização em tempo real de voz sobre IP.

7.4.28.Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

7.5.Controle por políticas de firewall

7.5.1.Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.
7.5.2.O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.
7.5.3.As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.
7.5.4.Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
7.5.5.Controle de políticas por países via localização por IP.
7.5.6.Suporte a objetos e regras IPV6.
7.5.7.Suporte a objetos e regras *multicast*.

7.6.Prevenção de ameaças

7.6.1.Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, *Anti-Malware* e Firewall de Proteção Web (WAF) integrados no próprio *appliance* de Firewall ou entregue em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.
7.6.2.Deve realizar a inspeção profunda de pacotes (DPI deep packet inspection) para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).
7.6.3.As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.
7.6.4.Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;
7.6.5.Deve suportar granularidade nas políticas de IPS Antivírus e *Anti-Malware*, possibilitando a criação de diferentes politicas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;
7.6.6.A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.
7.6.7.A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.
7.6.8.Deve ter proteção em tempo real contra novas ameaças criadas.
7.6.9.Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.
7.6.10.Deve permitir o bloqueio de vulnerabilidades.
7.6.11.Deve permitir o bloqueio de *exploits* conhecidos.
7.6.12.Deve detectar e bloquear o tráfego de rede que busque acesso a contact command e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.
7.6.13.Deve incluir proteção contra-ataques de negação de serviços.
7.6.14.Ser imune e capaz de impedir ataques básicos como: *SYN flood, ICMP flood, UDP Flood*, etc.
7.6.15.Suportar bloqueio de arquivos por tipo.
7.6.16.Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
7.6.17.Os eventos devem identificar o país de onde partiu a ameaça.
7.6.18.Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.

7.6.19.O firewall de aplicação Web (WAF) deverá ter a função de reverse proxy, com a função de URL hardening realizando deep-linking e prevensão dos ataques de path traversal ou directory traversal.
7.6.20.O firewall de aplicação Web (WAF) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.
7.6.21.O firewall de aplicação Web (WAF) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parametros de performance do WAF e permissão e bloqueio de ranges de IP.
7.6.22.Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente. Proteção pelo menos contra os seguintes ataques, mas não limitado a: SQL injection e Cross-site scripting.

7.7.Controle e proteção de aplicações

7.7.1.Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.
7.7.2.Deve de-criptografar/criptografar nos protocolos TLS 1.2 e 1.3;
7.7.3.Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.
7.7.4.Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/ SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.
7.7.5.Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website).
7.7.6.O escaneamento de micro app deverá ser habilitado via console gráfica (GUI) e via comando de linha (CLI).
7.7.7.Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.
7.7.8.Atualizar a base de assinaturas de aplicações automaticamente.
7.7.9.Reconhecer aplicações em IPv6.
7.7.10.Limitar a banda usada por aplicações (*traffic shaping*).
7.7.11.Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários.

7.7.12.Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.
7.7.13.Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

7.8.Controle e proteção web

7.8.1.Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.
7.8.2.Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a checagem de páginas em HTTPS.
7.8.3.Deve de-criptografar/criptografar nos protocolos TLS 1.2 e 1.3;
7.8.4.Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;
7.8.5.Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, Radius, *E-directory* e base de dados local;
7.8.6.Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
7.8.9.Possuir pelo menos 90 categorias de URLs;
7.8.10.Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
7.8.11.Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;
7.8.12.Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;
7.8.13.Suportar a criação categorias de URLs customizadas;
7.8.14.Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.
7.8.15.Permitir a customização de página de bloqueio;
7.8.16.Suportar a inclusão nos logs do produto de informações das atividades dos usuários;
7.8.17.Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.
7.8.18.Deve realizar caching do conteúdo web;
7.8.19.Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

7.9.Identificação de usuários

7.9.1.Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.
7.9.2.Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).

7.9.3.Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
7.9.4.Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.
7.9.5.Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.
7.9.6.Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

7.10.**Qualidade de serviço - QOS**

7.10.1.Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.
7.10.2.A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.
7.10.3.Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado.
7.10.4.Suportar priorização *Real-Time* de protocolos de voz (VoIP).

7.11.**Redes virtuais privadas – VPN**

7.11.1.Suportar VPN Site-to-Site e Cliente-to-Site.
7.11.2.Suportar IPsec VPN.
7.11.3.Suportar SSL VPN.
7.11.4.Suportar L2TP e PPTP.
7.11.5.Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.
7.11.6.Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL para estações Windows.
7.11.7.Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.
7.11.8.Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, HTTP, HTTPS, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.
7.11.9.A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).
7.11.10.Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.
7.11.11.Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
7.11.12.Suportar autenticação via AD/LDAP, Token e base de usuários local;
7.11.13.Permitir estabelecer um túnel SSL VPN com uma solução de autienticação via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local;

8.SOLUÇÃO ANTISPAM PARA CORREIO ELETRÔNICO (GATEWAY DE E-MAIL) – ITEM 12

8.1.A Solução para Proteção de Gateway de E-mail deve integrar a captura eficiente de spams com baixa taxa de categorização das mensagens como falsos positivos, Implementado como gateway de e-mails, deve proteger e-mails e mensagens instantâneas contra vírus, spams, phishing, botnets e outros e-mails indesejados. Deve incorporar recursos flexíveis para o gerenciamento de spams e atualizações automatizadas de filtros.

8.2.O Gateway AntiSpam deve suportar os seguintes requisitos mínimos:

8.2.1.Função de Relay SMTP (Simple Mail Transfer Protocol), com recurso de antispam;
8.2.2.Capacidade de throughput de 4.000 (quatro mil) conexões SMTP simultâneas;
8.2.3.Capacidade de atendimento ao tráfego de e-mail gerado a partir xxx (xxx) caixas postais de correio eletrônico, com taxa média de XXX (XXX) mensagens encaminhadas por hora;
8.2.4.Controle de sessões SMTP por meio de limite de tráfego de mensagens baseado em endereços IP, sub-redes IP, domínio e reputação do emissor;
8.2.5.Inspeção e bloqueio de mensagens baseados em tamanho de mensagem, volume de mensagens por período, número de destinatários por mensagem, número de destinatários por hora, destinatários inválidos, número de mensagens por conexão e número de conexões simultâneas por endereço IP;
8.2.6.Implementação da tecnologia SPF (Sender Policy Framework), de modo a evitar que outros domínios enviem e-mails não autorizados em nome de um domínio;
8.2.7.Implementação da tecnologia DKIM (Domain Keys Identified Mail), de modo a prover mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas;
8.2.8.Implementação de recursos de verificação de DNS reverso para validação de domínio;
8.2.9.Filtragem de conteúdo de e-mails por meio de assinaturas para corpo e anexos de mensagens, heurística, filtro de reputação, URLs e filtros anti-phishing;
8.2.10.Tratamento de mensagens com anexos contendo vírus, possibilitando o encaminhamento da mensagem sem o anexo infectado, bloqueio da mensagem e alerta ao destinatário do ocorrido;
8.2.11.Detecção de arquivos anexos, baseada em tipo, nome, extensão e formato MIME (Multipurpose Internet Mail Extensions);
8.2.12.Detecção de anexos compactados, incluindo formatos ZIP e RAR, permitindo definir a ação a ser executada;
8.2.13.Detecção de anexos criptografados, permitindo definir a ação a ser executada;
8.2.14.Detecção de reputação de links que estejam dentro do corpo de mensagens;
8.2.15.Implementação de recurso de quarentena por usuário, integrado e autenticado no Microsoft Active Directory;
8.2.16.Implementação de recurso de envio de notificação periódica para usuários acerca de mensagens de spam e em quarentena;
8.2.17.Implementação de recurso que permita o usuário administrar a sua própria quarentena;
8.2.18.Implementação de recurso de cadastro de lista negra branca pelo próprio usuário;
8.2.19.Implementação de configuração para bloqueio, encaminhamento, marcação e quarentena pelo próprio usuário;
8.2.20.Implementação de inserção de carimbo no assunto de mensagens e de texto no corpo de mensagens;
8.2.21.Gerenciamento por CLI (Command-line interface), SSH (Secure Shell), WebUI (WEB User Interface) via HTTPS (Secure Hypertext Transfer Protocol) e console gráfica centralizada;
8.2.22.Gerenciamento com perfis de acessos distintos para administração de funcionalidades, acesso a logs e emissão de relatórios;
8.2.23.Gerenciamento com recurso de informações estatísticas de fluxo de tráfego, incluindo quantidade de conexões, throughput e desempenho dos serviços;

8.2.24.Gerenciamento com recurso de emissão de relatórios, incluindo informações de quantidade de conexões, endereços IP, quantidade de e-mails.

8.3.Deve possuir recurso de sandbox integrada ao Gateway de AntiSpam, devendo detectar as seguintes ameaças:

8.3.1.Integração perfeita com sua solução de segurança de gateway de e-mail;
8.3.2.Proteção contra APTs de ransomware, malware desconhecido e ataques direcionados;
8.3.3.Deve possuir relatórios granulares de incidentes;
8.3.4.Deve possuir integração total no painel de solução de gateway e-mail;
8.3.5.Deve inspeciona executáveis e documentos contendo conteúdo executável, incluindo:
8.3.5.1.Executáveis do Windows (incluindo .exe, .com e .dll);
8.3.5.2.Documentos do Word (incluindo .doc, docx , docm e .rtf);
8.3.5.3.Documentos em PDF;
8.3.5.4.Arquivos contendo qualquer um dos tipos de arquivo listados acima (ZIP, BZIP, GZIP, RAR, TAR, LHA / LZH, 7Z, Gabinete da Microsoft);
8.3.6.Deve realizar a análise de comportamento de malware dinâmico executando arquivos em ambientes reais;
8.3.7.Possuir relatórios detalhados de arquivos maliciosos e capacidade de liberação dos arquivos no console de gerenciamento;

8.4.Treinamento – Capacitação – ITEM 13

8.4.1.Para garantir o pleno funcionamento da Solução de Segurança Corporativa, é essencial que a equipe da Contratante, em conjunto com a equipe de Administração venha a ser capacitada para a execução dos serviços em sua plenitude dentro dos requisitos exigidos pelo fabricante.
8.4.2.Será considerado curso ofertado pela própria CONTRATANTE, não sendo obrigatório Treinamento Oficial.
8.4.3.A CONTRATANTE poderá solicitar o treinamento para qualquer número de pessoas até o máximo previsto em contrato, inclusive para apenas 1 (uma) pessoa.
8.4.4.O Treinamento será ministrado nas dependências ou on-line;
8.4.5.Para tal, deverão ser ofertados treinamentos para cada um dos itens envolvidos e mencionados na solução de Segurança;
8.4.6.Carga horária de no mínimo vinte horas;

ANEXO B - ACORDO DE NÍVEL DE SERVIÇO

1. OBJETIVO

1.1. O Acordo de Nível de Serviço define os níveis de qualidade esperados na prestação do serviço e as respectivas supressões no pagamento, se for o caso, de fornecimento, aquisição, manutenção e garantia de Solução Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia e suporte e transferência de conhecimento para atendimento das necessidades da contratante.

1.2. Caso não seja atingido o nível de qualidade esperado na prestação do serviço o valor mensal a ser pago à CONTRATADA será reduzido.

1.3. O prazo de carência para adaptação e início por meio de ANS será de 30 (trinta) dias.

1.4. Descrição dos Níveis de Serviços de Garantia do Produto:

1.4.1. A CONTRATADA deverá fornecer garantia da solução pelo prazo contratado, contado a partir da emissão do Termo de Recebimento não se limitando ao término da vigência contratual;

1.4.2. Deverá ser oferecido suporte direto do fabricante, com possibilidade de abertura de chamados diretamente a ele em regime de 24x7 para resolução de problemas;

1.4.3. A garantia da solução deverá prover, durante o prazo discriminado no Termo de Referência obrigatoriamente:

1.4.3.1. Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

1.4.3.2. Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, ou se, mesmo não se tratando de substituição, fica caracterizada descontinuidade dos softwares fornecidos;

1.4.3.3. Eventuais correções dos softwares fornecidos (patches), incluindo a correção de eventuais falhas (bugs) de software reportadas pela contratante, que prejudique o ambiente de produção;

1.4.3.4. Acesso à base de conhecimento e a fóruns da solução no site do fabricante pelos servidores da contratante.

1.4.5. As manutenções corretivas, por solicitação expressa da CONTRATANTE à CONTRATADA, e preventiva, por solicitação da CONTRATADA a CONTRATANTE, serão realizadas dentro dos seguintes limites:

1.4.5.1. No caso de manutenções preventivas, o horário do atendimento deverá ser compreendido entre 9h00 e 18h00, em dias úteis (5x9h);

1.4.5.2. No caso de manutenções corretivas, o horário de atendimento será de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

1.4.6. O início do atendimento não poderá ultrapassar o prazo de 4 (quatro) horas, contadas a partir da solicitação feita pela CONTRATANTE. Entende-se por início do atendimento a proposta de uma solução para o problema.

1.4.7. O término da correção do problema não poderá ultrapassar:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 4 horas deve ter um técnico do fornecedor On-site ou remotamente.	Em até 12 horas
		Em até 2 horas. Um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone.	Entrega da Solução pelo fabricante em até 7 dias.
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 8 horas deve ter um técnico do fornecedor On-site ou remotamente.	Em até 16 horas
		Em até 4 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada.	Entrega da Solução pelo fabricante em até 14 dias.
Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Em até 12 horas deve ter um técnico do fornecedor On-site ou remotamente.	Em até 24 horas
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 20 dias ou na próxima atualização do Software

Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 72 horas
		No mesmo dia ou no próximo dia útil comercial	Entrega da Solução pelo fabricante em até 20 dias ou considerado para as próximas atualizações do Software

1.4.8. Será exigido o fornecimento de suporte on-site ou remoto por meio de central de atendimento telefônico 0800 ou e-mail.

1.4.9. Relatório de Acompanhamento de Nível de Serviço Mínimo:

1.4.9.1. O ressarcimento ao erário, por ocasião da aplicação das glosas referentes ao Nível de Serviço Mínimo, deverá ser executado mediante o preenchimento de Documento de Arrecadação Estadual (DAE), podendo ser substituído por outro instrumento legal, em nome do órgão contratante e pago até o último dia útil do mês subsequente a data de aplicação do Nível de Serviço Mínimo;

1.4.9.2. É garantido a CONTRATADA o direto à ampla defesa frente aos resultados da apuração do Nível de Serviço Mínimo, bem como a apresentação de justificativas que se fizerem necessárias;

1.4.9.3. As justificativas aceitas pelo gestor e pelo fiscal do contrato poderão anular a incidência de glosas e advertências na aplicação do Nível de Serviço Mínimo.

1.5. Nível de Serviço Mínimo

1.5.1. O Nível de Serviço Mínimo para este certame, será dado pela **Tabela I** a seguir:

1.5.1.1 Atendimento de chamados

PERCENTUAL DOS CHAMADOS COM ATRASO	TEMPO DE ATRASO PARA RESOLUÇÃO DOS CHAMADOS EM HORAS ÚTEIS	MEDIDAS CORRETIVAS
Até 5%	Tempo de atraso de 12h	aceito
	12h < tempo de atraso de 28h	advertência
	28 < tempo de atraso de 40h	Glosa de 1% do valor do equipamento por unidade atendida neste prazo
	Tempo de atraso > 40h	Sanções de que trata o modelo de gestão do contrato deste documento
	Tempo de atraso de 12h	advertência

5% a 10%	12h < tempo de atraso de 28h	Glosa de 1% do valor do equipamento por unidade atendida neste prazo
	28 < tempo de atraso de 40h	Glosa de 3% do valor do equipamento por unidade atendida neste prazo
	Tempo de atraso > 40h	Sanções de que trata o modelo de gestão do contrato deste documento
10% a 20%	Tempo de atraso de 12h	Glosa de 1% do valor do equipamento por unidade atendida nesta prazo
	12h < tempo de atraso de 28h	Glosa de 3% do valor do equipamento por unidade atendida neste prazo
	28 < tempo de atraso de 40h	Glosa de 5% do valor do equipamento por unidade atendida neste prazo
	Tempo de atraso > 40h	Sanções de que trata o modelo de gestão do contrato deste documento
20% a 30%	Tempo de atraso de 12h	Glosa de 3% do valor do equipamento por unidade atendida neste prazo
	12h < tempo de atraso de 28h	Glosa de 5% do valor do equipamento por unidade atendida neste prazo
	28 < tempo de atraso de 40h	Glosa de 8% do valor do equipamento por unidade atendida neste prazo
	Tempo de atraso > 40h	Sanções de que trata o modelo de gestão do contrato deste documento

Tabela I - Atendimento de chamados

1.5.2. A **Tabela I** representa a relação entre o percentual dos chamados atendidos fora dos prazos, o tempo gasto além do prazo definido, em horas úteis, para resolução do chamado e as respectivas sanções administrativas aplicáveis para cada caso.

1.5.3. As penalidades referentes aos tempos de atendimento são aplicadas da seguinte forma: valor do equipamento atendido vezes o número de equipamentos atendidos dentro do intervalo estabelecido na **Tabela I**, e para atraso superior às 40h úteis ou mais de 30% dos chamados resolvidos com atraso, aplicar-se-á as sanções definidas no modelo de gestão do contrato deste documento.

1.5.4. O Nível de Serviço Mínimo para este certame para apresentação do Relatório de Acompanhamento de Nível de Serviço Mínimo será dado pela **Tabela II** a seguir:

1.5.4.1. Apresentação do relatório

AÇÃO	DIAS ÚTEIS DE ATRASO NA ENTREGA	MEDIDAS CORRETIVAS

Apresentação do Relatório de Acompanhamento de Nível de Serviço Mínimo	Atraso ≤ 05 dias	Advertência
	05 dias < atraso ≤ 10 dias	Advertência Glosa de 0,25% sobre o valor do contrato por dia de atraso
	10 dias < atraso ≤ 30 dias	Advertência Glosa de 0,1 % sobre o valor do contrato por dia de atraso Glosa de 2% sobre o valor do contrato
	Atraso > 40 dias	Sanções de que trata o modelo de gestão do contrato deste documento

Tabela II - Apresentação de Relatório

1.5.5. Para efeitos de apuração dos níveis de serviço mínimos exigidos, utilizar-se-á o Relatório de Acompanhamento de Nível de Serviço Mínimo definido no item 1.4.

1.5.5.1. Poderão ser utilizadas as Ordens de Serviço para apuração ou conferência dos Níveis de Serviços Mínimos prestados.

1.5.6. No processo de aplicação de Glosas em razão do Nível de Serviço Mínimo é assegurado o direito ao contraditório e ampla defesa.

1.5.7. Glosas advindas do Nível de Serviço Mínimo que também poderão ser recolhidas em qualquer agência integrante da Rede Arrecadadora, por meio de Documento de Arrecadação Estadual (DAE), a ser preenchido de acordo com instruções fornecidas pela CONTRATANTE.

ANEXO C – ÓRGÃOS PARTICIPANTES

	Órgão/Entidade
1	**ETICE** - Empresa de Tecnologia da Informação do Ceará - Av. Pontes Vieira, 220 - São João do Tauape. CEP: 60.130-240. Fortaleza-CE.

ANEXO D - MODELO DE GESTÃO DO CONTRATO

1. MODELO DE GESTÃO DO CONTRATO

1.2. O CONTRATANTE, por meio de representantes nomeados por ato específico, fiscalizará a execução do contrato, não importando essa fiscalização em redução ou supressão da responsabilidade da CONTRATADA por eventual erro, falha ou omissão, exceto se decorrentes de determinações emanadas da Etice, das quais a CONTRATADA tenha discordado por escrito.

1.3. Para isso, o CONTRATANTE registrará em relatório as deficiências verificadas na execução dos serviços, encaminhando notificações à CONTRATADA, para a imediata correção das irregularidades apontadas, sem prejuízo da aplicação das penalidades previstas neste documento.

1.4. Objetivando assegurar a ETICE eficiente coordenação, a CONTRATADA obriga-se a indicar um representante e seu substituto eventual, para responder, perante o CONTRATANTE pelo gerenciamento técnico e operacional do contrato, até o total cumprimento das obrigações assumidas.

1.5. Cada bem/serviço só será aceito após os seus respectivos aceites provisório e definitivo.

1.6. O aceite provisório de cada bem/serviço é de caráter técnico e atesta que os bens foram fornecidos, para posterior análise das conformidades de qualidade baseadas nos critérios de aceitação. É realizado pelo responsável para o acompanhamento e fiscalização do contrato da solução.

1.7. Já o aceite definitivo tem por finalidade comprovar a adequação dos bens/serviços fornecidos conforme os requisitos estabelecidos nos termos contratuais. É realizado por servidor ou comissão designada pela autoridade competente.

2. CONDIÇÕES DE SUPORTE, GARANTIA E MANUTENÇÃO

2.1. Detalhamento das atividades de Suporte

2.1.1. O suporte técnico deverá ser prestado para cada solução aderida e deverá ser acionado em caso de qualquer indisponibilidade da solução, devendo haver o atendimento "on-site" ou remotamente, se requerido pelo CONTRATANTE, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações	Em até 4 horas deve ter um técnico do fornecedor On-site ou remotamente.	Em até 12 horas

	relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 2 horas. um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou remotamente	Entrega da Solução pelo fabricante em até 7 dias.
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 8 horas deve ter um técnico do fornecedor On-site ou remotamente.	Em até 16 horas
		Em até 4 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada.	Entrega da Solução pelo fabricante em até 14 dias.
Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Em até 12 horas deve ter um técnico do fornecedor On-site ou remotamente.	Em até 24 horas
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 20 dias ou na próxima atualização do Software
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos:	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 72 horas

	O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou	No mesmo dia ou no próximo dia útil comercial	Entrega da Solução pelo fabricante em até 20 dias ou considerado para as próximas atualizações do Software

2.1.2. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao CONTRATANTE, às providências que serão adotadas para a solução do chamado;

2.1.3. Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;

2.1.4. Os serviços de atendimento de garantia para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados);

2.1.5. O fornecedor emitirá relatório sempre que solicitado pelo CONTRATANTE, em papel e em arquivo eletrônico, preferencialmente em arquivo texto, com informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período, incluindo:

2.1.5.1. Quantidade de ocorrências (chamados) registradas no período;

2.1.5.2. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;

2.1.5.3. Data e hora de abertura;

2.1.5.4. Data e hora de início e conclusão do atendimento;

2.1.5.5. Identificação do técnico do CONTRATANTE que registrou o chamado;

2.1.5.6. Identificação do técnico do CONTRATANTE que atendeu o chamado da garantia;

2.1.5.7. Descrição do problema;

2.1.5.8. Descrição da solução;

2.1.5.9. Informações sobre eventuais escalações;

2.1.5.10. Resumo com a lista de chamados concluídos fora do prazo de solução estabelecido;

2.1.5.11. Total de chamados no mês e o total acumulado até a apresentação do relatório;

2.1.6. As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da proponente;

2.1.7. Nos casos em que as manutenções necessitarem de paradas da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda à aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

2.1.8. O proponente deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os

pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do Complexo Central de Tecnologia do CONTRATANTE, caso requeiram;

2.1.9. O relatório deve ser assinado por representante do CONTRATANTE, responsável pelo acompanhamento do serviço, que se obriga a acompanhar a execução das manutenções;

2.1.10. Por questão de segurança, o servidor nunca deverá ser removido da dependência do CONTRATANTE com os discos rígidos. Nesse caso, o disco rígido do equipamento deverá ser removido e entregue ao primeiro gestor da dependência do CONTRATANTE;

2.1.11. Durante o período de garantia o fornecedor executará, sem ônus adicionais, correções de falhas (bugs) de hardware e software;

2.1.12. Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada;

2.2. Canais de Atendimento

2.2.1. Será disponibilizado canal de atendimento e chamado técnico 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de canal telefônico 0800 ou e-mail;

2.2.2. Em caso de indisponibilidade do canal de atendimento disponibilizado, os chamados técnicos poderão ser abertos via email ou "website" do fabricante ou telefone;

2.3. Garantia

2.3.1. O fornecedor concederá à CONTRATANTE garantia integral durante 24 (vinte e quatro) meses, “on-site” ou remotamente com atendimento 24 horas por dia e sete dias por semana, a contar da data de homologação do produto, contra qualquer defeito ou problema em toda a solução, incluindo avarias no transporte dos equipamentos até o local de entrega, mesmo ocorrida sua aceitação/aprovação pelo contratante;

2.3.2. A garantia inclui a substituição dos equipamentos/produtos defeituosos no prazo máximo de 45 (quarenta e cinco) dias corridos, a contar da comunicação do fato, sem qualquer ônus para o contratante. Neste caso, as novas unidades empregadas na substituição das defeituosas ou danificadas deverão ter prazo de garantia igual ou superior ao das substituídas;

2.3.3. O fornecedor garante por, no mínimo, 24 (vinte quatros) meses o fornecimento dos componentes de hardware e software, para manutenções, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas. Caso haja neste período a descontinuidade de fabricação dos componentes, deve ser também garantida à total compatibilidade dos itens substitutos com os originalmente fornecidos;

2.3.4. Durante o período de garantia, deve ser efetuada manutenção preventiva, em intervalos predeterminados e de acordo com critérios prescritos pelo CONTRATANTE, destinada a reduzir a probabilidade de falha ou a degradação do funcionamento da solução, para tanto, o proponente deve fornecer, quando da assinatura do contrato, cronograma com previsão das manutenções preventivas;

2.4. Manutenção

2.4.1. Manutenção corretiva será efetuada sempre que a solução apresente falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado;

2.4.2. As manutenções preventivas e corretivas serão de responsabilidade do fornecedor, sem custos adicionais ao CONTRATANTE;

2.4.3. Durante o período de garantia, qualquer componente que apresente defeito ou mau funcionamento, sem indicação de solução, deve ser substituído imediatamente;

ANEXO II - CARTA PROPOSTA

À

Central de Licitações do Estado do Ceará.

Ref.: Pregão Eletrônico nº 20190012 – ETICE.

A proposta encontra-se em conformidade com as informações previstas no edital e seus Anexos.

1. Identificação do licitante:

a) Razão Social:

b) CPF/CNPJ e Inscrição Estadual:

c) Endereço completo:

d) Representante Legal (nome, nacionalidade, estado civil, profissão, RG, CPF, domicílio):

e) Telefone, celular, fax, e-mail:

2. Condições Gerais da Proposta:

- A presente proposta é válida por _____ (_____) dias, contados da data de sua emissão.
- O objeto contratual terá garantia de _____(_____) _____ para os itens 9, 10 e 11 do grupo 1.

3. Formação do Preço:

GRUPO_____

ITEM	ESPECIFICAÇÃO	UNIDADE	QTDE	VALOR (R$)	
				UNITÁRIO	TOTAL

VALOR GLOBAL R$:

Valor por extenso (_____)

DECLARO, sob as sanções administrativas cabíveis, inclusive as criminais e sob as penas da lei, que toda documentação anexada ao sistema são autênticas.

Local e data

Assinatura do representante legal

(Nome e cargo)

ANEXO III - MINUTA DA ATA DE REGISTRO DE PREÇOS

ATA DE REGISTRO DE PREÇOS Nº ___ /20__.

PREGÃO ELETRÔNICO Nº 20190012.

PROCESSO Nº 09551772/2019.

Aos __ dias do mês de _____ de 20__, na sede da Empresa de Tecnologia da Informação do Ceará - ETICE, foi lavrada a presente Ata de Registro de Preços, conforme deliberação da Ata do Pregão Eletrônico nº 20190012 - ETICE do respectivo resultado homologado, publicado no Diário Oficial do Estado em __/__/20__, às fls ____, do Processo nº **09551772/2019***,* que vai assinada pelo titular da Empresa de Tecnologia da Informação do Ceará - ETICE - gestora do Registro de Preços, pelos representantes legais dos detentores do registro de preços, todos qualificados e relacionados ao final, a qual será regida pelas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DO FUNDAMENTO LEGAL

1.1. O presente instrumento fundamenta-se:

I. No Pregão Eletrônico nº 20190012 – ETICE.

II. Nos termos do Decreto Estadual nº 32.824, de 11/10/2018, publicado D.O.E de 11/10/2016.

III. Na Lei Federal nº 13.303, de 30.6.2016.

CLÁUSULA SEGUNDA - DO OBJETO

A presente Ata tem por objeto o Registro de preços, visando futuras e eventuais **serviços de fornecimento, aquisição, manutenção de Solução Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Empresa de Tecnologia da Informação do Ceará**, cujas especificações e quantitativos encontram-se detalhados no Anexo I - Termo de Referência do Pregão Eletrônico nº 20190012 - ETICE, que passa a fazer parte desta Ata, com as propostas de preços apresentadas pelos fornecedores classificados em primeiro lugar, conforme consta nos autos do Processo nº **09551772/2019**.

Subcláusula Única - Este instrumento não obriga a Administração a firmar contratações, exclusivamente por seu intermédio, podendo realizar licitações específicas, obedecida a legislação pertinente, sem que, desse fato, caiba recurso ou indenização de qualquer espécie aos detentores do registro de preços, sendo-lhes assegurado a preferência, em igualdade de condições.

CLÁUSULA TERCEIRA - DA VALIDADE DA ATA DE REGISTRO DE PREÇOS

A presente Ata de Registro de Preços terá validade pelo prazo de 12 (doze) meses, contados a partir da data da sua publicação ou então até o esgotamento do quantitativo nela registrado, se este ocorrer primeiro.

CLÁUSULA QUARTA - DA GERÊNCIA DA ATA DE REGISTRO DE PREÇOS

Caberá a ETICE o gerenciamento deste instrumento, no seu aspecto operacional e nas questões legais, em conformidade com as normas do Decreto Estadual nº 32.824/2018, publicado no D.O.E de 11/10/2018.

CLÁUSULA QUINTA - DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

Em decorrência da publicação desta Ata, a ETICE poderá firmar contratos com os fornecedores com preços registrados.

Subcláusula Primeira - O prestador de serviço terá o prazo de 5 (cinco) dias úteis, contados a partir da convocação, para a assinatura do contrato. Este prazo poderá ser prorrogado uma vez por igual período, desde que solicitado durante o seu transcurso e, ainda assim, se devidamente justificado e aceito.

Subcláusula Segunda - Na assinatura do contrato será exigida a comprovação das condições de habilitação exigidas no edital, as quais deverão ser mantidas pela contratada durante todo o período da contratação.

CLÁUSULA SEXTA - DAS OBRIGAÇÕES E RESPONSABILIDADES

Os signatários desta Ata de Registro de Preços assumem as obrigações e responsabilidades constantes no Decreto Estadual de Registro de Preços nº 32.824/2018.

Subcláusula Primeira - Competirá a ETICE na qualidade de gestor do Registro de Preços, o controle e administração do SRP, em especial, as atribuições estabelecidas nos incisos I ao VII, do art. 17, do Decreto Estadual n° 32.824/2018.

Subcláusula Segunda - Caberá a ETICE, as atribuições que lhe são conferidas nos termos dos incisos I a V do art. 18, do Decreto Estadual n° 32.824/2018.

Subcláusula Terceira - O detentor do registro de preços, durante o prazo de validade desta Ata, fica obrigado a:

a) Atender os pedidos efetuados pela ETICE, bem como aqueles decorrentes de remanejamento de quantitativos registrados nesta Ata, durante a sua vigência.

b) Executar os serviços ofertados, por preço unitário registrado, nas quantidades indicadas pela ETICE do Sistema de Registro de Preços.

c) Responder no prazo de até 5 (cinco) dias a consultas do órgão gestor de Registro de Preços sobre a pretensão de órgão/entidade não participante.

d) Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta, observando o prazo mínimo exigido pela Administração.

CLÁUSULA SÉTIMA - DOS PREÇOS REGISTRADOS

Os preços registrados são os preços unitários ofertados nas propostas dos detentores de preços desta Ata, os quais estão relacionados no Mapa de Preços dos itens, anexo único deste instrumento e servirão de base para futuras execuções de serviços, observadas as condições de mercado.

CLÁUSULA OITAVA - DA REVISÃO DOS PREÇOS REGISTRADOS

Os preços registrados só poderão ser revistos nos casos previstos no art. 23, do Decreto Estadual n° 32.824/2018.

CLÁUSULA NONA - DO CANCELAMENTO DO REGISTRO DE PREÇOS

Os preços registrados na presente Ata, poderão ser cancelados de pleno direito, nas situações previstas no art. 25, e na forma do art. 26, ambos do Decreto Estadual n° 32.824/2018.

CLÁUSULA DÉCIMA - DAS CONDIÇÕES PARA A EXECUÇÃO

Os serviços que poderão advir desta Ata de Registro de Preços serão formalizadas por meio de instrumento contratual a ser celebrado entre a ETICE e o prestador de serviço.

Subcláusula Primeira - Caso o prestador de serviço classificado em primeiro lugar, não cumpra o prazo estabelecido pela ETICE, ou se recuse a executar o serviço, terá o seu registro de preço cancelado, sem prejuízo das demais sanções previstas em lei e no instrumento contratual.

Subcláusula Segunda - Neste caso, a ETICE convocará sucessivamente por ordem de classificação, os demais prestadores de serviços.

CLÁUSULA DÉCIMA PRIMEIRA - DA EXECUÇÃO E DO RECEBIMENTO

Subcláusula Primeira - Quanto à execução

a) O objeto contratual deverá ser executado em conformidade com as especificações estabelecidas neste instrumento, em um prazo máximo de 90 (noventa) dias úteis contado a partir do recebimento da ordem de serviço ou instrumento hábil.

b) Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de execução, e aceitos pela ETICE, não serão considerados como inadimplemento contratual.

Subcláusula Segunda - Quanto ao recebimento:

a) PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela contratante.

b) DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após verificação da qualidade e da quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e, consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

CLÁUSULA DÉCIMA SEGUNDA - DO PAGAMENTO

O pagamento advindo do objeto da Ata de Registro de Preços será proveniente dos recursos do (s) próprios órgão (s)/entidades participante (s) e será efetuado mensalmente até 30 (trinta) dias a contar da data da apresentação da Nota Fiscal/Fatura devidamente atestada pelo gestor da contratação, mediante crédito em conta-corrente em nome da contratada, exclusivamente no Banco Bradesco S/A, conforme Lei nº 15.241, de 06 de dezembro de 2012.

Subcláusula Primeira - A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

Subcláusula Segunda - Não será efetuado qualquer pagamento à CONTRATADA, em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

Subcláusula Terceira - É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações do Anexo I - Termo de Referência do edital do Pregão Eletrônico nº 20190012 - ETICE.

Subcláusula Quarta - No caso de atraso de pagamento, desde que a contratada não tenha concorrido de alguma forma para tanto, serão devidos pela contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

Subcláusula Quinta - O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos, N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento, I = Índice de compensação financeira = 0,00016438 e VP = Valor da prestação em atraso.

Subcláusula Sexta - Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:

a) Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União, Certidão Negativa de Débitos Estaduais, Certidão Negativa de Débitos Municipais, Certificado de Regularidade do FGTS - CRF, Certidão Negativa de Débitos Trabalhistas - CNDT.

Subcláusula Sétima - Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, autenticada por cartório competente ou por servidor da Administração, ou publicação em órgão da imprensa oficial. Caso a documentação tenha sido emitida pela internet, só será aceita após a confirmação de sua autenticidade.

CLÁUSULA DÉCIMA TERCEIRA - DAS SANÇÕES ADMINISTRATIVAS

Subcláusula Primeira - Pela inexecução total ou parcial do contrato, a contratante poderá, garantida a prévia defesa, aplicar a contratada, nos termos do art. 83 da Lei nº 13.303/2016, as seguintes penalidades:

a) Advertência

b) Multas, estipuladas na forma a seguir:

b.1) Multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento) pela inobservância do prazo fixado para apresentação da garantia.

b.2) Multa diária de 0,3% (três décimos por cento), no caso de atraso na execução do objeto contratual até o 30º (trigésimo) dia, sobre o valor da nota de empenho ou instrumento equivalente e rescisão contratual, exceto se houver justificado interesse público em manter a avença, hipótese em que será aplicada apenas a multa.

b.3) Multa diária de 0,5% (cinco décimos por cento), no caso de atraso na execução do objeto contratual superior a 30 (trinta) dias, sobre o valor da nota de empenho ou instrumento equivalente. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior.

b.4) Multa de 0,1% (um décimo por cento), sobre o valor da nota de empenho ou instrumento equivalente, em caso de descumprimento das demais cláusulas contratuais, elevada para 0,3% (três décimos por cento), em caso de reincidência.

b.5) Multa de 20% (vinte por cento), sobre o valor do contrato, no caso de desistência da execução do objeto ou rescisão contratual não motivada pela contratante.

c) Suspensão temporária de participação em licitação e impedimento de contratar com a entidade sancionadora, por prazo não superior a 2 (dois) anos.

CLÁUSULA DÉCIMA QUARTA - DA FRAUDE E DA CORRUPÇÃO

O detentor de preços registrado deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o

processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos desta cláusula, definem-se as seguintes práticas:

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

b) "prática fraudulenta": a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato.

c) "prática conluiada": esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos.

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

e) "prática obstrutiva":

(1) Destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista nesta cláusula.

(2) Atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

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

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

Subcláusula Terceira - A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas em Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

CLÁUSULA DÉCIMA QUINTA - DO FORO

Fica eleito o foro do município de Fortaleza, capital do Estado do Ceará, para conhecer das questões relacionadas com a presente Ata que não possam ser resolvidas pelos meios administrativos.

Assinam esta Ata, os signatários relacionados e qualificados a seguir, os quais firmam o compromisso de zelar pelo fiel cumprimento das suas cláusulas e condições.

Signatários:

Órgão Gestor	Nome do Titular	Cargo	CPF	RG	Assinatura

Detentores do Registro de Preços	Nome do Representante	Cargo	CPF	RG	Assinatura

ANEXO ÚNICO DA ATA DE REGISTRO DE PREÇOS Nº ___ /20__ - MAPA DE PREÇOS DOS SERVIÇOS

Este documento é parte da Ata de Registro de Preços acima referenciada, celebrada entre a Empresa de Tecnologia da Informação do Ceará - ETICE e o Prestador de Serviço, cujos preços estão a seguir registrados por item, em face da realização do Pregão Eletrônico nº 20190012 - ETICE.

Item	Cód Item	Especificação do Item	Fornecedores Por Ordem de Classificação	Qtde	Unidade	Preço Registrado do Item(R$)	Valor Total (R$)

ANEXO IV - MINUTA DO CONTRATO

CONTRATO Nº ____ / _____.

PROCESSO Nº 095517722019 - ETICE.

CONTRATO QUE ENTRE SI CELEBRAM A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ - ETICE E (O) A _____, ABAIXO QUALIFICADOS, PARA O FIM QUE NELE SE DECLARA.

A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ - ETICE, situada na _____, inscrita no CNPJ sob o nº _____, doravante denominada CONTRATANTE, neste ato representada pelo _____, (nacionalidade), portador da Carteira de Identidade nº _____, e do CPF nº _____, residente e domiciliada(o) em (Município - UF), na _____, e a _____, com sede na _____, CEP: _____, Fone: _____, inscrita no CPF/CNPJ sob o nº _____, doravante denominada CONTRATADA, representada neste ato pelo _____, (nacionalidade), portador da Carteira de Identidade nº _____, e do CPF nº _____, residente e domiciliada(o) em (Município - UF), na _____, têm entre si justa e acordada a celebração do presente contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA - DA FUNDAMENTAÇÃO

1.1. O presente contrato tem como fundamento o edital do Pregão Eletrônico n° 20190012 - ETICE e seus anexos, os preceitos do direito público, e a Lei Federal nº 13.303/2016, o Regulamento de Interno de Licitações e Contratos da ETICE e, ainda, outras leis especiais necessárias ao cumprimento de seu objeto.

CLÁUSULA SEGUNDA - DA VINCULAÇÃO AO EDITAL E A PROPOSTA

2.1. O cumprimento deste contrato está vinculado aos termos do edital do Pregão Eletrônico nº 20190012 - ETICE e seus Anexos, e à proposta da CONTRATADA, os quais constituem parte deste instrumento, independente de sua transcrição.

CLÁUSULA TERCEIRA - DO OBJETO

3.1. Constitui objeto deste contrato o **serviço de fornecimento, aquisição, manutenção de Solução Integrada e Gerenciamento Seguro da Informação em ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades da Empresa de Tecnologia da Informação do Ceará**, de acordo com as especificações e quantitativos previstos no Anexo I - Termo de Referência do Edital e na proposta da CONTRATADA.

CLÁUSULA QUARTA - DO REGIME DE EXECUÇÃO

4.1. O objeto dar-se-á sob o regime de execução indireta: **Empreitada por preço unitário**.

CLÁUSULA QUINTA - DO VALOR E DO REAJUSTAMENTO DO PREÇO

5.1. O valor contratual global importa na quantia de R$ _____ (_____), sujeito a reajustes, desde que observado o interregno mínimo de 01 (um) ano, a contar da apresentação da proposta.

5.1.1. Caso o prazo exceda a 01 (um) ano, o preço contratual será reajustado, utilizando a variação do índice nacional de preços ao Consumidor Amplo - IPCA, calculado pelo Instituto Brasileiro de Geografia e Estatística - IBGE.

CLÁUSULA SEXTA - DO PAGAMENTO

6.1. O pagamento advindo do objeto da Ata de Registro de Preços será proveniente dos recursos da ETICE e será efetuado mensalmente até 30 (trinta) dias a contar da data da apresentação da Nota Fiscal/Fatura devidamente atestada pelo gestor da contratação, mediante crédito em conta-corrente em nome da contratada, exclusivamente no Banco Bradesco S/A, conforme Lei nº 15.241, de 06 de dezembro de 2012.

6.1.1. A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

6.2. Não será efetuado qualquer pagamento à CONTRATADA, em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

6.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações do Anexo I - Termo de Referência do edital do Pregão Eletrônico n° 20190012 - ETICE.

6.4. No caso de atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, serão devidos pela CONTRATANTE encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

6.4.1. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos, N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento, I = Índice de compensação financeira = 0,00016438 e VP = Valor da prestação em atraso.

6.5. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:

6.5.1. Certidão Conjunta Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União, Certidão Negativa de Débitos Estaduais, Certidão Negativa de Débitos Municipais, Certificado de Regularidade do FGTS - CRF, Certidão Negativa de Débitos Trabalhistas - CNDT.

6.6. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, autenticada por cartório competente ou por servidor da Administração, ou publicação em órgão da imprensa oficial. Caso a documentação tenha sido emitida pela internet, só será aceita após a confirmação de sua autenticidade.

CLÁUSULA SÉTIMA - DOS RECURSOS ORÇAMENTÁRIOS

7.1. As despesas decorrentes da contratação serão provenientes dos recursos _____.

CLÁUSULA OITAVA - DO PRAZO DE VIGÊNCIA E DE EXECUÇÃO

8.1. Os prazos de vigência e de execução contratual serão de 24 (vinte e quatro) meses, a partir da celebração do contrato conforme disposto no art. 71 da Lei nº 13.303/2016.

8.2. Os prazos de vigência e de execução poderão ser prorrogados nos termos do que dispõe o art. 71 e 81 da Lei Federal nº 13.303/2016.

18.3. A publicação resumida deste contrato dar-se-á nos termos do § 2º do art. 51 da Lei nº 13.303/2016.

CLÁUSULA NONA - DA GARANTIA CONTRATUAL

9.1. A garantia prestada, de acordo com o estipulado no edital, será restituída e/ou liberada após o cumprimento integral de todas as obrigações contratuais e, quando em dinheiro, será atualizada monetariamente, conforme dispõe o § 4º, do art. 70, da Lei Federal nº 13.303/2016. Na ocorrência de acréscimo contratual de valor, deverá ser prestada garantia proporcional ao valor acrescido, nas mesmas condições inicialmente estabelecidas.

CLÁUSULA DÉCIMA - DA EXECUÇÃO E DO RECEBIMENTO

10.1. Quanto à execução:

10.1.1. O objeto contratual deverá ser executado em conformidade com as especificações e locais indicados no Anexo C do Termo de Referência do Edital.

10.1.2. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de execução, e aceitos pela CONTRATANTE, não serão considerados como inadimplemento contratual.

10.2. Quanto ao recebimento:

10.2.1. PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela CONTRATANTE.

10.2.2. DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após a verificação da qualidade e quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

CLÁUSULA DÉCIMA PRIMEIRA - DAS OBRIGAÇÕES DA CONTRATADA

11.1. Executar o objeto em conformidade com as condições deste instrumento.

11.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

11.3. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

11.4. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

11.5. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

11.6. Refazer, substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo fixado pelo(s) órgão(s)/entidade(s) participante(s) do SRP (Sistema de Registro de Preços), contado da sua notificação.

11.7. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

11.8. Providenciar a substituição de qualquer empregado que esteja a serviço da contratante, cuja conduta seja considerada indesejável pela fiscalização da contratante.

11.9. Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, e demais normas do Ministério do Trabalho, relativos a segurança e a medicina do trabalho, bem como a Legislação correlata em vigor a ser exigida.

11.10. Disponibilizar nos termos da Lei nº 15.854, de 24/09/2015, vagas de empregos a presos em regime semiaberto, aberto, em livramento condicional e egressos do sistema prisional e aos jovens do sistema socioeducativo entre 16 e 18 anos, que estejam cumprindo medida de semiliberdade. Caso a execução contratual não necessite, ou necessite de 5 (cinco) ou menos trabalhadores, a reserva de vagas será facultativa.

11.10.1. Encaminhar mensalmente, respectivamente, à CISPE/SAP e à SPS, a folha de frequencia dos presos e egressos e/ou jovens do sistema socieducativo, contemplados com a reserva de vagas. Caso a contratação não esteja obrigada a disponibilizar vagas nos termos da Lei nº 15.854, de 24/09/2015 ficará dispensada do envio da folha de frequência.

11.12. Fornecer os equipamentos novos e de primeiro uso e os softwares deverão está em suas últimas versões e com atualização sem custo no período de garantia.

CLÁUSULA DÉCIMA SEGUNDA - DAS OBRIGAÇÕES DA CONTRATANTE

12.1. Solicitar a execução do objeto à contratada através da emissão de Ordem de Fornecimento/ Serviço.

12.2. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal nº 13.303/2016.

12.3. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

12.4. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

12.5. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.

12.6. Aplicar as penalidades previstas em lei e neste instrumento.

CLÁUSULA DÉCIMA TERCEIRA - DA FISCALIZAÇÃO

13.1. A execução contratual será acompanhada e fiscalizada pelo (a) _____, especialmente designado (a) para este fim pela CONTRATANTE, de acordo com o estabelecido no art. 67, da Lei Federal nº 8.666/1993, doravante denominada simplesmente de GESTOR (A).

CLÁUSULA DÉCIMA QUARTA - DAS SANÇÕES ADMINISTRATIVAS

14.1. Pela inexecução total ou parcial do contrato, a contratante poderá, garantida a prévia defesa, aplicar a contratada, nos termos do art. 83 da Lei nº 13.303/2016, as seguintes penalidades:

14.1.1. Advertência.

14.1.2. Multas, estipuladas na forma a seguir:

a) Multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento) pela inobservância do prazo fixado para apresentação da garantia.

b) Multa diária de 0,3% (três décimos por cento), no caso de atraso na execução do objeto contratual até o 30º (trigésimo) dia, sobre o valor da nota de empenho ou instrumento equivalente e rescisão contratual, exceto se houver justificado interesse público em manter a avença, hipótese em que será aplicada apenas a multa.

c) Multa diária de 0,5% (cinco décimos por cento), no caso de atraso na execução do objeto contratual superior a 30 (trinta) dias, sobre o valor da nota de empenho ou instrumento equivalente. A aplicação da presente multa exclui a aplicação da multa prevista na alínea anterior.

d) Multa de 0,1% (um décimo por cento), sobre o valor da nota de empenho ou instrumento equivalente, em caso de descumprimento das demais cláusulas contratuais, elevada para 0,3% (três décimos por cento), em caso de reincidência.

e) Multa de 20% (vinte por cento), sobre o valor do contrato, no caso de desistência da execução do objeto ou rescisão contratual não motivada pela contratante.

14.1.1.3. Suspensão temporária de participação em licitação e impedimento de contratar com a entidade sancionadora, por prazo não superior a 2 (dois) anos.

CLÁUSULA DÉCIMA QUINTA - DA FRAUDE E DA CORRUPÇÃO

15.1. A contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos desta cláusula, definem-se as seguintes práticas:

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

b) “prática fraudulenta”: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato.

c) “prática conluiada”: esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos.

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

e) “prática obstrutiva”:

(1) Destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista nesta cláusula.

(2) Atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

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

15.3. Considerando os propósitos dos itens acima, o contratado deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

15.4. A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas em Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

CLÁUSULA DÉCIMA SEXTA - DA SUBCONTRATAÇÃO

16.1. Será admitida a subcontratação se previamente aprovada pela contratante, e que não constitua o escopo principal do objeto, restrita, contudo, ao percentual máximo de 30% (trinta por cento) da contratação.

16.2. A subcontratação de que trata esta cláusula, não exclui a responsabilidade da contratada perante a contratante quanto à qualidade técnica da obra ou do serviço prestado, não constituindo portanto qualquer vínculo contratual ou legal da contratante com a subcontratada.

16.3. A contratada ao requerer autorização para subcontratação de parte do objeto, deverá comprovar perante a Administração a regularidade jurídico/fiscal e trabalhista de sua subcontratada.

CLÁUSULA DÉCIMA SÉTIMA - DA RESCISÃO CONTRATUAL

17.1. A inexecução total ou parcial deste contrato será causa para sua rescisão, em cumprimento ao inciso VII do art. 69 da Lei Federal nº 13.303/16 e regulamento interno de licitações.

17.2. Este contrato poderá ser rescindido a qualquer tempo pela CONTRATANTE, mediante aviso prévio de no 30 (trinta) dias, nos casos das rescisões decorrentes de razões de interesse público

de alta relevância e amplo conhecimento desde que justificado, sem que caiba à CONTRATADA direito à indenização de qualquer espécie.

CLÁUSULA DÉCIMA OITAVA - DO FORO

18.1. Fica eleito o foro do município de Fortaleza, capital do Estado do Ceará,para dirimir quaisquer questões decorrentes da execução deste contrato, que não puderem ser resolvidas na esfera administrativa.

E, por estarem de acordo, foi mandado lavrar o presente contrato, que está visado pela Assessoria Jurídica da CONTRATANTE, e do qual se extraíram 3 (três) vias de igual teor e forma, para um só efeito, as quais, depois de lidas e achadas conforme, vão assinadas pelos representantes das partes e pelas testemunhas abaixo.

Local e data

(nome do representante) (nome do representante)

CONTRATANTE CONTRATADO(A)

Testemunhas:

(nome da testemunha 1) (nome da testemunha 2)

RG: RG:

CPF: CPF:

Visto:

(Nome do(a) procurador(a)/assessor(a) jurídico(a) da CONTRATANTE)

ANEXO V - MODELO DE DECLARAÇÃO DE AUTENTICIDADE DOS DOCUMENTOS

(PAPEL TIMBRADO DO PROPONENTE)

DECLARAÇÃO

(nome /razão social) _____, inscrita no CNPJ nº_____,por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da Carteira de Identidade nº_____e CPF nº _____, DECLARA, sob as sanções administrativas cabíveis, inclusive as criminais e sob as penas da lei, que toda documentação anexada ao sistema são autênticas.

Local e data

Assinatura do representante legal

(Nome e cargo)