Boletim Eletrônico - SEI em 24/07/2020

FUNDAÇÃO JORGE DUPRAT FIGUEIREDO DE SEGURANÇA E MEDICINA DO TRABALHO
Rua Capote Valente, 710, - Bairro Pinheiros, São Paulo/SP, CEP 05409-002
Telefone: - http://www.fundacentro.gov.br

EDITAL Nº 01/2020/2020

Processo nº 47648.000293/2020-35

PREGÃO ELETRÔNICO Nº 01/2020

Torna-se público que a Fundação Jorge Duprat Figueiredo de Segurança e Medicina do Trabalho, Fundacentro, por meio do Serviço de Compras, realizará licitação na modalidade PREGÃO, na forma ELETRÔNICA, **com o critério de julgamento menor preço por grupo**, sob a forma de execução indireta, no regime de empreitada por preço global, nos termos da Lei nº 10.520, de 17 de julho de 2002,da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: 06 de agosto de 2020
Horário: 10h30 - horário de Brasília
Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br

DO OBJETO

O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de serviços de tecnologia da informação e comunicação em renovação, suporte e manutenção de licenças antivírus, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

A licitação será realizada em grupo único, formados por dois itens, conforme tabela abaixo e constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

Grupo 1					
Item	**Descrição**	**Catser**	**Quantidade (unidade)**	**Valor máximo unitário**	**Valor máximo total**
1	Renovação de Licença de Software Unificado de Gerenciamento de Antivírus CEB (Complete Endpoint Protection Business)	350949	400	R$ 243,94	R$ 97.576,00
2	Renovação das Licenças, Suporte e Manutenção de antivírus para desktops e servidores EDR (McAfee Endpoint Detection & Response)	350949	400	R$ 176,46	R$ 70.584,00

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

Cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB.

DOS RECURSOS ORÇAMENTÁRIOS

As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da União para o exercício de 2020, na classificação abaixo:

Gestão/Unidade: 264001

Fonte: 0100, 0280 ou 0144

Programa de Trabalho: 173303

Elemento de Despesa: 33904006

PI: 22000401113

DO CREDENCIAMENTO

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

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

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

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

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

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

DA PARTICIPAÇÃO NO PREGÃO

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

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

Não poderão participar desta licitação os interessados:

proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

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

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

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

que estejam sob falência, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação;

entidades empresariais que estejam reunidas em consórcio;

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

instituições sem fins lucrativos (parágrafo único do art. 12 da Instrução Normativa/SEGES nº 05/2017)

É admissível a participação de organizações sociais, qualificadas na forma dos arts. 5º a 7º da Lei 9.637/1998, desde que os serviços objeto desta licitação se insiram entre as atividades previstas no contrato de gestão firmado entre o Poder Público e a organização social (Acórdão nº 1.406/2017- TCU-Plenário), mediante apresentação do Contrato de Gestão e dos respectivos atos constitutivos.

Será permitida a participação de cooperativas, desde que apresentem modelo de gestão operacional adequado ao objeto desta licitação, com compartilhamento ou rodízio das atividades de coordenação e supervisão da execução dos serviços, e desde que os serviços contratados sejam executados obrigatoriamente pelos cooperados, vedando-se qualquer intermediação ou subcontratação.

Em sendo permitida a participação de cooperativas, serão estendidas a elas os benefícios previstos para as microempresas e empresas de pequeno porte quando elas atenderem ao disposto no art. 34 da Lei nº 11.488, de 15 de junho de 2007.

Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

> detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou
>
> de autoridade hierarquicamente superior no âmbito do órgão contratante.

Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto n.º 7.203, de 04 de junho de 2010);

Nos termos do art. 7° do Decreto n° 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança

neste órgão contratante.

Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

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

nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

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

que está ciente e concorda com as condições contidas no Edital e seus anexos;

que cumpre plenamente os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

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

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

que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

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

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

que cumpre os requisitos do Decreto n. 7.174, de 2010, estando apto a usufruir dos critérios de preferência.

a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto no Decreto nº 7.174, de 2010.

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

DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio desse documento.

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

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

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.

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

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

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.

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

PREENCHIMENTO DA PROPOSTA

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

Valor unitário e total do item;

Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

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

Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo deste Edital;

A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1° do artigo 57 da Lei n° 8.666, de 1993.

Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2° da IN SEGES/MPDG n. 5/2017.

A empresa é a única responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;

cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.

Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses, devendo o licitante ou contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.

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

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

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

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

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

O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

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

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

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

Também será desclassificada a proposta que identifique o licitante.

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

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

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

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

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

O lance deverá ser ofertado pelo total do lote.

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

O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

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.

Encerrado o prazo previsto no item anterior, o sistema abrirá oportunidade para que o autor 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 que será sigiloso até o encerramento deste prazo.

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

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

Não havendo lance final fechado e classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada para que os demais licitantes, até no 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, observando-se, após, o item anterior.

Poderá o pregoeiro, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender as exigências de habilitação

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

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

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

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

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

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

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

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

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

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

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

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

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

prestados por empresas brasileiras;

prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

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

Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas ou os lances empatados.

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

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

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

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

Será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

DA ACEITABILIDADE DA PROPOSTA VENCEDORA

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

A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio da Planilha de Custos e Formação de Preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme anexo deste Edital.

A Planilha de Custos e Formação de Preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de 2 (duas) horas, contado da solicitação do Pregoeiro, com os respectivos valores adequados ao lance vencedor e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MPDG n. 5/2017, que:

não estiver em conformidade com os requisitos estabelecidos neste edital;

contenha vício insanável ou ilegalidade;

não apresente as especificações técnicas exigidas pelo Termo de Referência;

apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018-TCU – Plenário), desconto menor do que o mínimo exigido, ou que apresentar preço manifestamente inexequível.

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

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

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

Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MPDG N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas,

devendo apresentar as provas ou os indícios que fundamentam a suspeita.

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

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

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

Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se as planilhas de custo readequadas com o valor final ofertado.

Todos os dados informados pelo licitante em sua planilha deverão refletir com fidelidade os custos especificados e a margem de lucro pretendida.

O Pregoeiro analisará a compatibilidade dos preços unitários apresentados na Planilha de Custos e Formação de Preços com aqueles praticados no mercado em relação aos insumos e também quanto aos salários das categorias envolvidas na contratação;

Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço.

O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

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

Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

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

DA HABILITAÇÃO

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

SICAF;

Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União - TCU;

Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c” e “d” acima pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoesapf.apps.tcu.gov.br/)

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

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

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

O licitante será convocado para manifestação previamente à sua desclassificação.

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

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

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

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

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

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

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

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

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

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

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

Ressalvado o disposto do item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação nos itens a seguir, para fins de habilitação.

Habilitação jurídica:

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

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

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

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

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

decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

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

Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Regularidade fiscal e trabalhista:

prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

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

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

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

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

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

caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

Qualificação Econômico-Financeira:

certidão negativa de falência expedida pelo distribuidor da sede do licitante;

balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

Caso o licitante seja cooperativa, tais documentos deverão ser acompanhados da última auditoria contábil-financeira, conforme dispõe o artigo 112 da Lei nº 5.764, de 1971, ou de uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

LG = Ativo Circulante + Realizável a Longo Prazo / Passivo Circulante + Passivo Não Circulante

SG = Ativo Total / Passivo Circulante + Passivo Não Circulante

LC = Ativo Circulante / Passivo Circulante

As empresas, , que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10 (dez por cento) do valor total estimado da contratação ou do item pertinente.

Qualificação Técnica:

Os critérios de Qualificação técnica estão listados no Termo de referência.

Em relação às licitantes cooperativas será, ainda, exigida a seguinte documentação complementar:

A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764 de 1971;

A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

O registro previsto na Lei n. 5.764/71, art. 107;

A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764/71 ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

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

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

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

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

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

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

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

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

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

DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 2 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

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

apresentar a planilha de custos e formação de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.

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

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

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

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

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

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

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

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

DOS RECURSOS

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

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

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

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

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

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

Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

DA REABERTURA DA SESSÃO PÚBLICA

A sessão pública poderá ser reaberta:

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

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

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

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

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

DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

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

DA GARANTIA DE EXECUÇÃO

Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência.

DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido no prazo de 5 (cinco) dias, a contar da data de seu recebimento.

O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

O prazo de vigência da contratação é de 24 (vinte e quatro) meses, prorrogável conforme previsão no instrumento contratual e no termo de referência.

Previamente à contratação a Administração realizará consulta ao Sicaf para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a

assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

DO REAJUSTAMENTO EM SENTIDO GERAL

As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

DO PAGAMENTO

As regras acerca do pagamento são as estabelecidas no Termo de Referência, anexo a este Edital.

DAS SANÇÕES ADMINISTRATIVAS

Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

não assinar a ata de registro de preços, quando cabível;

apresentar documentação falsa;

deixar de entregar os documentos exigidos no certame;

ensejar o retardamento da execução do objeto;

não mantiver a proposta;

cometer fraude fiscal;

comportar-se de modo inidôneo;

As sanções do item acima também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

Multa de até 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com

ou sem a participação de agente público.

Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

As penalidades serão obrigatoriamente registradas no SICAF.

As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

A impugnação poderá ser realizada por forma eletrônica, pelo e-mail scp@fundacentro.gov.br ou por petição dirigida ou protocolada no endereço Rua Capote Valente, 710, Pinheiros, São Paulo – SP.

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

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

Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

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

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

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

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

DAS DISPOSIÇÕES GERAIS

Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

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

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

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

As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

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

O Edital está disponibilizado, na íntegra, nos endereços eletrônicos www.fundacentro.gov.br e www.comprasgovernamentais.gov.br.

Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I - Termo de Referência;

ANEXO II - Minuta de Termo de Contrato.

TATIANA GONÇALVES	FELIPE MEMOLO PORTELA
Pregoeira	Ordenador de despesas - Presidente

Documento assinado eletronicamente por **Tatiana Goncalves**, **Chefe de Serviço**, em 17/07/2020, às 16:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Felipe Memolo Portela**, **Presidente**, em 20/07/2020, às 17:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.fundacentro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0066599** e o código CRC **27A629D9**.

ANEXO I - Termo de Referência

Documento SEI 0046770

ANEXO II - Minuta de Termo de Contrato

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ...../....., QUE FAZEM ENTRE SI A FUNDAÇÃO JORGE DUPRAT FIGUEIREDO DE SEGURANÇA E MEDICINA DO TRABALHO – FUNDACENTRO E A EMPRESA .....

A Fundação Jorge Duprat Figueiredo de Segurança e Medicina do Trabalho – FUNDACENTRO, com sede à ....., cidade de ....., Estado de ..... inscrita no CNPJ sob o nº ....., neste ato representada por seu Presidente, Senhor ....., nomeado pela Portaria nº ....., de ..... de ..... de 20..., publicada no DOU de ..... de ..... de ....., portador da Matrícula Funcional nº ....., doravante denominada CONTRATANTE, e o(a) ..... inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ..... doravante designada CONTRATADA, neste ato representada pelo(a) Sr. (a) ....., portador(a) da Carteira de Identidade nº ....., expedida pela (o) ....., e CPF nº ....., tendo em vista o que consta no Processo nº ..... e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 9.507, de 21 de setembro de 2018, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019 e da Instrução Normativa SEGES/MPDG nº 5, de 26 de maio de 2017 e suas alterações, resolvem celebrar o presente Termo de Contrato, decorrente do nº ...../20...., mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO

O objeto do presente instrumento é a contratação de serviços de ....., que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital.

Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

Objeto da contratação:

Item	Descrição do Item	Unidade de Medida	Quantidade	Valor Unitário
1				
2				

CLÁUSULA SEGUNDA – VIGÊNCIA

O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, isto é, 24 (vinte e quatro) meses, com início na data da última assinatura dos contraentes, podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, desde que haja autorização formal da autoridade competente e seja observado o disposto no Anexo IX da IN SEGES/MP nº 05/2017, atentando, em especial para o cumprimento dos seguintes requisitos:

Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;

Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

Seja comprovado que o valor do contrato permanece economicamente vantajoso para a Administração;

Haja manifestação expressa da contratada informando o interesse na prorrogação;

Seja comprovado que a contratada mantém as condições iniciais de habilitação.

A CONTRATADA não tem direito subjetivo à prorrogação contratual.

A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

CLÁUSULA TERCEIRA – PREÇO

O valor total da contratação é de R$ ..... (.....)..

No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

O valor acima é meramente estimativo, de forma que os pagamentos devidos à CONTRATADA dependerão dos quantitativos de serviços efetivamente prestados.

CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 20...., na classificação abaixo:

Gestão/Unidade:

Fonte:

Programa de Trabalho:

Elemento de Despesa:

PI:

No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

CLÁUSULA QUINTA – PAGAMENTO

O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Termo de Referência e no Anexo XI da IN SEGES/MPDG n. 5/2017.

CLÁUSULA SEXTA – REAJUSTAMENTO DE PREÇOS EM SENTIDO AMPLO

As regras acerca do reajustamento de preços em sentido amplo do valor contratual (reajuste em sentido estrito e/ou repactuação) são as estabelecidas no Termo de Referência, anexo a este Contrato.

CLÁUSULA SÉTIMA – GARANTIA DE EXECUÇÃO

Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência.

CLÁUSULA OITAVA – MODELO DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

O modelo de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados, a disciplina do recebimento do objeto e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

CLÁUSULA DÉCIMA – SANÇÕES ADMINISTRATIVAS

As sanções relacionadas à execução do contrato são aquelas previstas no Termo de Referência, anexo do Edital.

CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

O presente Termo de Contrato poderá ser rescindido:

por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

O termo de rescisão, sempre que possível, será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

Relação dos pagamentos já efetuados e ainda devidos;

Indenizações e multas.

CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES

É vedado à CONTRATADA:

caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

interromper a execução contratual sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN/SEGES/MPDG nº 05, de 2017.

A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

CLÁUSULA DÉCIMA SEXTA – FORO

É eleito o Foro da Seção Judiciária de São Paulo – Justiça Federal para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato depois de lido e achado em ordem, vai assinado eletronicamente pelos contraentes.

Representante legal da CONTRATANTE

Representante legal da CONTRATADA

Criado por juan.pereira, versão 3 por juan.pereira em 17/07/2020 15:36:29.

FUNDAÇÃO JORGE DUPRAT FIGUEIREDO DE SEGURANÇA E MEDICINA DO TRABALHO
Rua Capote Valente, 710, - Bairro Pinheiros, São Paulo/SP, CEP 05409-002
Telefone: e Fax: @fax_unidade@ - http://www.fundacentro.gov.br

TERMO DE REFERÊNCIA

Processo nº 47648.000293/2020-35

OBJETO

Neste Termo de Referência estão contemplados os requisitos necessários para contratação e execução de serviços descritos em conformidade com a IN nº 01, de 04 de abril de 2019 da Secretaria de Governo Digital (SGD) do Ministério da Economia (ME), que dispõe sobre as contratações de bens e serviços de Tecnologia da Informação e Comunicação.

Considera-se que os serviços do objeto a ser contratado são comuns, nos termos do parágrafo único do Art. 1º da Lei 10.520 de 2002.

As quantidades e respectivos códigos dos itens seguem especificados na tabela a seguir:

Item	Descrição do Item (Objeto)	CATMAT/CATSER	Quantidade	Unidade de Medida
1	Renovação de Licença de Software Unificado de Gerenciamento de Antivírus CEB (Complete Endpoint Protection Business)	350949	400	unidade
2	Renovação das Licenças, Suporte e Manutenção de antivírus para desktops e servidores EDR (McAfee Endpoint Detection & Response)	350949	400	unidade

A presente contratação adotará como regime de execução a Empreitada por Preço Global.

O prazo de vigência do contrato é de 24 (vinte e quatro) meses, podendo ser prorrogado por interesse das partes.

JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

MOTIVAÇÃO DA CONTRATAÇÃO

É imprescindível o uso continuado de ferramenta antivírus, pois a mesma combate malwares (vírus, trojan, worm, entre outros), proporcionando atualização frequente no combate às pragas digitais. A proteção das estações de trabalho atua nos arquivos existentes e em dispositivos removíveis como pendrive.

A proteção dos servidores de dados também atua nos recursos citados no item anterior, acrescido de ferramentas específicas e serviços que são executados nos mesmos.

A proteção do correio eletrônico se direciona para cada caixa postal existente no servidor Microsoft Exchange. Dessa forma, é possível resguardar cada e-mail (caixa postal) com o antivírus, coibindo a entrada e saída de possíveis malwares.

As licenças de antivírus da FUNDACENTRO venceram no terceiro trimestre de 2019, o que evidencia a urgência da necessidade da contratação.

O SIN ampliou o portifólio de sistemas e servidores de aplicação para atendimento da missão da FUNDACENTRO nos últimos anos, como por exemplo: Rede SST, Moodle para Pós-Graduação, Servidores de homologação de sistemas, entre outros.

A atuação do antivírus também estará nos servidores de aplicação de missão crítica da FUNDACENTRO, dentre eles: Intranet, Portal, Pastas da Rede, E-mail.

Além disso, manter o antivírus nos desktops e notebooks aumenta a eficiência das análises de vulnerabilidade e consequente mitigação de malwares, bem como há adequação do sistema às novas características de maior performance da infraestrutura de TI. Também se observa com o uso de antivírus atualizado, aumento dos níveis de segurança da informação, bem como aumento da eficiência de monitoração de eventos de segurança relacionados à malwares e redução dos incidentes de segurança relacionados à malwares.

BENEFÍCIOS DIRETOS E INDIRETOS QUE RESULTARÃO DA CONTRATAÇÃO

O STIC ampliou o portifólio de sistemas e servidores de aplicação para atendimento da missão da FUNDACENTRO nos últimos anos, como por exemplo: SEI, Rede SST, Moodle para Pós-Graduação, Servidores de homologação de sistemas, entre outros

A atuação do antivírus também estará nos servidores de aplicação de missão crítica da FUNDACENTRO, dentre eles: Intranet, Portal, Pastas da Rede, E-mail

Aumentar a eficiência das análises de vulnerabilidade e consequente mitigação de malwares

Adequação do sistema às novas características de maior performance da infraestrutura de TI

Aumento dos níveis de segurança da informação

Aumento da eficiência de monitoração de eventos de segurança relacionados à malwares

Redução dos incidentes de segurança relacionados à malwares

CONEXÃO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO EXISTENTE

A descrição da solução como um todo partiu do Planejamento da Contratação, conforme minudenciado nos Estudos Preliminares, e abrange a prestação do serviço de antivírus para Sede/CTN e UD's. A contratação pleiteada teve como ponto de partida a proposta SIn.001.2019 no SGPA.

CRITÉRIOS AMBIENTAIS ADOTADOS (SUSTENTABILIDADE)

Os softwares devem ser fornecidos em meio digital, sem a necessidade de entrega de versões dos produtos em mídias, indo de encontro com os requisitos de TI Verde com a consequente não utilização de recursos não renováveis, como é o caso do plástico.

A documentação técnica deve ser fornecida em meio digital, com um descritivo completo do processo de implantação de cada produto ofertado, explicações sobre o registro e uso de licenças de software, forma de acesso ao site do fabricante para download da solução antivírus completa, assim como de seus upgrades e updates.

Não serão aceitas cópias impressas da documentação das licenças.

DESCRIÇÃO DA SOLUÇÃO

A descrição da solução como um todo, conforme minudenciado no Estudo Técnico Preliminar, abrange a contratação de empresa especializada para renovação de licença de antivírus para desktops, notebooks e servidores de aplicação da Sede/Centro Técnico Nacional (CTN) e Unidades Descentralizadas (UD's), incluindo serviços de configuração, implantação e suporte.

DA CLASSIFICAÇÃO DOS SERVIÇOS E FORMA DE SELEÇÃO DO FORNECEDOR

Trata-se de serviço comum de caráter continuado sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante licitação, na modalidade pregão, em sua forma eletrônica.

Os itens são compostos no mesmo lote devido à característica intrínseca de relacionamento entre eles.

A opção por lote único, nas licitações por empreitada de preço global, mesmo que em serviços distintos, ou serviços e materiais independentes, agrupados em um único lote, devem ser excepcionais, mas admissíveis quando, comprovada e justificadamente, houver inter-relação entre os serviços contratados, gerenciamento centralizado ou implicar em vantagem para a Administração, o que é o caso da presente contratação.

A interdependência das licenças e serviços ocorre nesta contratação, já que há uma impossibilidade dos mesmos estabelecerem por si só o limite de atuação entre as atividades e para que não haja prejuízo para a Administração em possíveis conflitos entre fornecedores dos softwares, tais como versões incompatíveis e implantação de software não gerenciado pela licitante vencedora do item específico.

Os serviços a serem contratados enquadram-se nos pressupostos do Decreto n° 9.507, de 21 de setembro de 2018, não se constituindo em quaisquer das atividades, previstas no art. 3º do aludido decreto, cuja execução indireta é vedada.

A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

Por tratar-se de serviço que requer do licitante vencedor conhecimento técnico especializado em face do grau de complexidade do objeto do certame, o licitante vencedor deverá entregar documento que comprove que o(s) técnico(s) que prestar(á)ão o suporte técnico da solução possua(m) certificação oficial da solução ofertada.

O documento de comprovação deverá ser entregue na assinatura do contrato, juntamente com documento oficial que comprove o vínculo empregatício entre os técnicos certificados e o licitante vencedor.

REQUISITOS DA CONTRATAÇÃO

Conforme Estudos Preliminares, os requisitos da contratação abrangem os itens que constam nesta subseção deste Termo de Referência (TR).

É obrigatória apresentação de declaração do licitante vencedor de que tem pleno conhecimento das condições necessárias para a prestação do serviço.

As obrigações da Contratada e Contratante estão previstas neste TR.

REQUISITOS GERAIS

Todas as licenças e componentes que compõem a solução deverão ser entregues com todos os impostos, taxas e demais custos inerentes ao fabricante e/ou distribuidor da solução, devidamente quitados.

Deverá ser utilizado o *Grant Number* (número de identificação) da FUNDACENTRO equivalente à renovação das licenças que permita fazer o download da solução antivírus completa, assim como de seus upgrades e updates.

Todas as licenças, referentes aos softwares e/ou drivers solicitados, devem estar em nome da Contratante, em modo definitivo (licenças perpétuas), não poderão ser cobrados quaisquer valores adicionais pelo seu uso, durante ou após o término do contrato.

Não serão admitidas versões “shareware” ou “trial”.

Todas as licenças e componentes que compõem a solução deverão ser entregues com todos os impostos, taxas e demais custos inerentes ao fabricante e/ou distribuidor da solução, devidamente quitados.

A contratada deverá apresentar comprovante de que é uma empresa autorizada pelo fabricante seja para o fornecimento de licenças e para a prestação de serviços de instalação, manutenção e suporte técnico;

NOTAS E ESCLARECIMENTOS

Para todos os itens de especificação, serão aceitas ofertas de qualquer componente de especificação diferente da solicitada, desde que comprovadamente iguale ou supere, individualmente, a qualidade, o desempenho, a operacionalidade, a ergonomia ou a facilidade no manuseio do originalmente especificado – conforme o caso, e desde que não cause, direta ou indiretamente, incompatibilidade com qualquer das demais especificações, ou desvantagem nestes mesmos atributos dos demais componentes ofertados.

A descrição do produto a ser ofertado deverá ser o da especificação própria da marca do equipamento, não o da transcrição (repetição) das especificações descritas no presente edital, salvo se esta for idêntica em sua integralidade com o requisitado pela FUNDACENTRO.

GARANTIA E SUPORTE

Durante o período de vigência do contrato, bem como os períodos de prorrogações a CONTRATADA deverá realizar a continuidade do suporte técnico e garantir a atualização tecnológica da solução na forma de atualizações de programas. As atualizações de programas deverão cobrir todos os programas de computador (software e firmware) adquiridos e incluir o fornecimento de correções (patches) e novas versões/revisões/distribuições (releases) assim que o fabricante as torne disponíveis. Entende-se por atualização de programas qualquer correção, pequena modificação, aperfeiçoamento (update), ou desenvolvimento de nova versão (upgrade) efetuado pelo fabricante para os produtos em questão.

A manutenção deverá ser prestada a contar da data de emissão do Termo de Recebimento Definitivo, 8 (oito) horas por dia, 5 (cinco) dias por semana, contemplando substituição de qualquer componente da solução em caso de defeito, nos prazos estabelecidos nesta especificação técnica visando dar continuidade, sem custo adicional para a FUNDACENTRO.

Suporte técnico com a finalidade de garantir o bom funcionamento da solução, a CONTRATADA deverá disponibilizar o serviço de gerenciamento remoto de todos os módulos envolvidos na solução, durante a vigência do Contrato, visando a continuidade dos serviços.

Os atendimentos dos chamados de suporte técnico poderão ser solucionados através de suporte por acesso remoto.

As atividades de suporte técnico e gerenciamento remoto da solução destinam-se a prover informação, assistência e orientação para: instalação, desinstalação, configuração, substituição e atualização de programas (software); aplicação de correções (patches) e atualizações de software; diagnósticos, avaliações e resolução de problemas; ajustes finos e customização da solução; características dos produtos; e demais atividades relacionadas à correta operação e funcionamento da solução da melhor maneira possível.

Os serviços de atualizações deverão ser finalizados no prazo de 30 (dez) dias úteis, após recebimento do licenciamento contratado

A garantia deverá englobar qualquer atividade relacionada ao funcionamento dos produtos, como manutenção evolutiva, preventiva e corretiva em software e nos serviços, sem nenhum ônus para a Contratante.

Durante o período de garantia é de responsabilidade da Contratada, a atualização de versões dos softwares fornecidos, mesmo que saiam de linha e não sejam mais suportados pelo fabricante.

A Contratada deverá disponibilizar para a FUNDACENTRO, sem custo adicional, as respectivas atualizações de versões e “releases” de todos os produtos fornecidos, durante o período de garantia e deverá prestar ao Contratante todo o suporte necessário para instalação e configuração das mesmas.

Durante o período de garantia de atualização técnica, a Contratada deverá entregar as revisões dos manuais técnicos e/ou documentação dos softwares licenciados, sem ônus adicionais para a FUNDACENTRO.

A Contratada garante ao Contratante que os produtos licenciados para uso não infringem quaisquer patentes, direitos autorais ou trade-secrets.

Caso os produtos licenciados venham a ser objeto de ação judicial em que se discuta a infringência de patentes, direitos autorais ou trade-secrets, a Contratada garante ao Contratante que assumirá a direção defesa em juízo, responsabilizando-se pelos honorários advocatícios, custas processuais, bem como por todo e qualquer prejuízo.

Especificação técnica do item 01 - Renovação de Licença de Software Unificado de Gerenciamento de Antivírus CEB (Complete Endpoint Protection Business)

Características Gerais da Solução

A solução deve contemplar as seguintes funcionalidades básicas, descritas a seguir:

Deve possuir suporte a arquiteturas 32-bits e 64-bits.

Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho

Deve suportar as seguintes plataformas clientes:

Windows 10;

Windows 8.1;

Windows 8;

Windows 7;

Deve suportar as seguintes plataformas servidores:

Windows Server 2016;

Windows Server 2012 R2;

Windows Server 2012;

Windows 2008 R2 (Standard/Enterprise);

Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:

Microsoft Hyper-V 2012 R2;

Vmware ESXi;

Vmware Player;

Vmware vShpere;

Vmware Workstation;

Toda a proteção deverá ser realizada através de um único agente de proteção com as funcionalidades descritas neste termo, não sendo aceitos plugins ou softwares adicionais para a composição do pacote.

O agente único deve compreender as seguintes funcionalidades:

Prevenção de Ameaças;

Firewall;

Controle Web;

Inteligência contra Ameaças;

Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:

Relatórios;

Dashboards;

Políticas;

Configuração;

Instalação/Desinstalação;

O cliente deve ser capaz de operar em modo autonomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente.

O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfix'es a partir de um servidor definido pelo administrador ou diretamente nos servidores da McAfee.

A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente;

A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;

A solução deve conter módulo capaz de proteger contra botnets, negação de serviço, executáveis não confiáveis e conexões web maliciosas;

A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)

A solução deve conter módulo capaz de garantir integração entre as soluções do fabricante proposto e entre fabricantes terceiros, compartilhando as informações do paciente dia zero para melhor mitigar novas ameças.

Este módulo deve estar público para o desenvolvimento da comunidade via Github;

Proteção Clientes Windows - Proteção de Ameaças

Prevenção de exploração:

Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).

Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.

Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.

Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;

Deve ser possível incluir exclusões por:

Processo: Nome; Caminho do Arquivo; Hash MD5

Módulo chamador: Nome; Caminho; Hash MD5; Signatário Digital

Proteção de acesso

Deve fornecer regras de proteção nativamente, ou seja definida pelo fabricante da solução, no mínimo, para:

Acesso remoto a pastas locais; Alteração políticas de direitos dos usuários; Alterar os registros de extensão dos arquivos; Criação de novos arquivos na pasta Arquivo de Programas; Criação de novos executáveis na pasta Windows; Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema; Criar ou Modificar remotamente arquivos ou pastas; Desativar o editor de registro e o gerenciador de tarefas; Executar arquivos das pastas do usuário; Execução de scripts pelo host de script do Windows; Instalar objetos de ajuda a navegação ou extensões de shell; Instalar novos CLSIDs, APPIDs e TYPELIBs; Modificar configurações de rede; Modificar configurações do Internet Explorer; Modificar processos principais do Windows; Navegadores iniciando programas da pasta de downloads; Registrar programas para execução automática.

As regras especificadas devem permitir o seu:

Bloqueio, ou

Informação, ou

Bloqueio e Informação;

Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parametros:

Processos: Nome do processo; Hash MD5; Assinatura Digital;

Usuário

Arquivos: Criação;Deletar;Executar;Alteração de permissão;Leitura;Renomear;Escrever;

Chave de Registro: Escrever;Criar;Deletar;Ler;Enumerar;Carregar;Substituir;Restaurar;Alterar permissão;

Valor de Registro: Ler;Criar;Deletar;

Processo: Qualquer acesso;Criar thread;Modificar;Terminar;Executar;

Deve permitir a criação de exclusões;

Varredura ao acessar

A Varredura deve ser passível de habilitação/desativação por opção do administrador;

Deve iniciar a proteção durante a inicialização do sistema operacional;

Deve ser capaz de realizar análise no setor de boot;

O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;

Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo;

Deve possibilitar ao administrador a análise de instaladores confiáveis;

Deve realizar análise durante copia entre pastas locais;

A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;

Deve permitir a configuração do nível de agressividade da análise entre:

Muito Baixo

Baixo

Médio

Alto

Muito Alto

Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo

administrador;

Deve realizar varredura quando o processo:

Ler o disco;

Gravar no disco;

Deixar a solução de proteção decidir;

Deve possibilitar análise em

Unidades de Rede;

Arquivos abertos para backup;

Arquivos compactados, por exemplo .jar;

Arquivos codificados (MIME)

Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;

Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

Limpar o arquivo;

Excluir o arquivo;

Negar acesso ao arquivo;

Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

Limpar o arquivo;

Excluir o arquivo;

Permitir acesso ao arquivo;

Negar acesso ao arquivo;

Deve possibilitar ao administrador a gestão de uma lista de exclusões;

Deve possuir módulo capaz de interceptar scripts destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;

Deve permitir a criação de listas de exclusão de URL's que não sofrerão interceptação e análise de scripts;

Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

Varredura sob demanda

Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.

Deve permitir a criação de repetição da tarefa.

Deve permitir definir a hora da execução da tarefa de análise;

Deve permitir a criação da tarefa de varredura de maneira aleatória;

Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.

Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:

Os locais da varredura, dentre eles:Memória para rootkits;Processos em execução;Arquivos registrados;Meu computador;Todas as unidades locais;Todas as unidades fixas;Todas as unidades removíveis;Todas as unidades mapeadas;Pasta inicial;Pasta de perfil do usuário;Pasta Windows;Pasta de arquivos de programas;Pasta temporária;Lixeira;Arquivo ou pasta especificada pelo administrador;Setor de inicialização (boot);Arquivos compactados;Arquivos MIME;

Os tipos de arquivos que serão analisados;

Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.

Áreas de exclusão que não deverão ser varridas;

Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada para a detecção de ameaças desconhecidas.

Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

Limpar o arquivo;

Excluir o arquivo;

Negar acesso ao arquivo;

Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

Limpar o arquivo;

Excluir o arquivo;

Permitir acesso ao arquivo;

Negar acesso ao arquivo;

Para minimizar o impacto ao usuário, a solução deve permitir:

Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;

Iniciar a varredura apenas quando o sistema estiver ocioso;

Permitir ao usuário retomar varreduras pausadas;

Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;

Proteção de Rede

O módulo de Firewall de Host deve incluir as seguintes capacidades:

Deve permitir a ativação/desativação do módulo de Firewall através da console;

Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura contra ataques dia zero;

Deve possuir um firewall de estação statefull bloqueando tráfego de entrada e controlando o tráfego de saída;

Deve possuir assinaturas de proteção para:

Arquivos

Chave de Registro

Processos

Serviços;

Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;

Deve ser possível bloquear trafego bridge;

Deve ser possível bloquear contra falsificação de IP (IP Spoofing)

O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;

Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;

Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações:

Nome

Nome do arquivo ou Caminho

Hash MD5

Assinador Digital

Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;

As conexões identificadas pelo Centro de Inteligência podem ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.

Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;

Deve permitir inspeção do protocolo FTP;

Deve ser possível bloquear trafego de protocolos não suportados;

O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.

O módulo de firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parametros:

Ação:Bloquear;Permitir

Direção:Ambas;Entrada;Saída

Protocolo:Qualquer protocolo;Protocolo IP(Ipv4;Ipv6;Protocolo Não-IP);Tipo de Conexão(Rede Sem Fio;Rede Cabeada;Rede Virtual);Especificação da Rede(Endereço IP;Subnet;Range;FQDN);Protocolo de Transporte(Todos;ICMP;ICMPv6;TCP;UDP;STP;GRE;IGMP;IPSEC AH;IPSEC ESP;Ipv6 in Ipv4;ISIS over Ipv4;L2TP); Agendamento(Dias da Semana;Hora Inicio;Hora Fim);Aplicações

Deve possuir as seguintes proteções:

Generic Buffer Overflow Protection;

Suspicious caller and caller validation;

Exploit Prevention

Access Protection;

Data Execution Protection

Generic Privilege Escalation Protection

Proteção Web

O modulo de Controle Web deve possuir as seguintes funcionalidades:

Deve permitir o bloqueio de browsers não suportados, dentre eles:

Opera

Safari for Windows;

Netscape

Maxthon

Flock;

Avant Browser;

Deepnet Explorer

PhaseOut

Deve permitir o controle de browsers suportados, dentre eles:

Chrome

Firefox

Internet Explorer

Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado.

Deve possuir, no mínimo, as seguintes categorias:

Browser Exploits; Download Maliciosos; Sites Maliciosos; Phishing; Pornografia; Hacking/Computer Crime; Spyware/Adware/Keyloggers; Anonymizer; Anonymizer Utilities; Alcohol; Blogs/Wiki; Business; Chat; Content Server; Dating;Dating/Social Networking; Digital Postcards; Discrimination; Drugs; Education; Entertainment; Extreme; Fashion; Finance; For Kids; Forum; Gambling; Game/Cartoon Violence; Games; General News; Government/Military; Gruesome Content; Health; Historical Revisionism; History; Humor/Comics; Illegal UK; Incidental Nudity; Information Security; Instant Messaging; Interactive Web Applications; Internet Radio/TV; Internet Services; Job Search; Major Global Religions; Marketing/Merchandising; Media Downloads; Media Sharing; Messaging; Mobile Phone; Moderated; Motor Vehicles; Non-Profit/Advocacy/NGO; Nudity; Online Shopping; P2P/File Sharing; Parked Domain; Personal Network Storage; Personal Pages; Pharmacy; Politics/Opinion; Portal Sites; Potential Criminal Activities; Potential Illegal Software; Potentially Unwanted Programs; Profanity; Professional Networking; Provocative Attire; Public Information; Real Estate; Recreation/Hobbies; Religion/Ideology; Remote Access; Residential IP Addresses; Resource Sharing; Restaurants; School Cheating Information; Search Engines; Sexual Materials; Shareware/Freeware; Social Networking; Software/Hardware; Spam URLs; Sports; Stock Trading; Streaming Media; Technical Information; Technical/Business Forums; Text Translators; Text/Spoken Only; Tobacco; Travel; Uncategorized; Usenet News; Violence; Visual Search Engine; Weapons; Web Ads; Web Mail; Web Meetings; Web Phone.

Deve ser possível bloquear um site conforme a sua classificação:

Alto Risco

Médio Risco

Não categorizado

Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;

Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;

Deve permitir a varredura de arquivos baixados da internet;

Deve ser possível excluir endereços IP da análise;

Deve permitir a busca segura para buscadores, dentre eles:

Google;

Yahoo

Bing;

Ask;

Deve bloquear links que direcionem para sites com alto risco.

Deve permitir a customização das mensagens apresentadas para o usuário;

Caso o módulo detecte que exista um McAfee Web Gateway na rede, deverá deixar a análise a cargo deste último.

Blindagem das estações de trabalho

O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas, aplicar o controle de execução (Blindagem da estação de trabalho) e realizar controle e auditoria sobre as alterações realizadas pelos usuários;

Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes.

Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão;

Ao detectar um executável, a solução deverá consultar o Centro de Inteligência do fabricante e esta deverá informar um nível de confidência (Bom, Mau ou Não Classificado);

Para o caso de problema com o envio de informações para o fabricante, este deverá possibilitar executar a tarefa por meio do servidor de reputação local;

Deve ser possível criar uma imagem base para a criação de uma política geral;

Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;

A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos;

Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:

Desabilitado: proteção desativada

Monitoramento: Monitora toda a atividade da Estação de Trabalho;

Atualização: a cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido;

Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA-1).

A solução deve suportar as seguintes modalidades de proteção:

Application Whitelisting: criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impadidas de serem executadas.

Application Blocking / Blacklisting: criação de uma lista de aplicações não autorizadas que não podem ser executadas.

Memory Protection: monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.

Change Control: Deve monitorar mudanças de arquivos e chaves de registro em tempo real.

Solução suporta criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.

Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação do aplicativo ou arquivo.

Suporta os mecanismos:

Application Code Protection: permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, etc) possam ser executados. Além disso, permite proteção contra adulterações de programas em Whitelist (ex.: arquivos do programa) e, opcionalmente, chaves de registros contra modificações em disco.

Memory Protection: permite proteção contra ataques e exploração de vulnerabilidades para os programas em Whitelist.

Suporta criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de Whitelist, através de:

Binário: binário específico identificado através de seu nome ou de algorítmo de verificação SHA-1.

Trusted Publisher: fornecedor específico, assinado digitalmente por um certificado de segurança emitido,

para este fornecedor, por uma Autoridade Certificadora (CA - Certificate Authority).

Trusted Installer: software instalado por um programa instalador específico, identificações por seu algorítmo de verificação, independentemente de sua origem.

Trusted Directories: pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.

Trusted Program / Authorized Updater: programas identificados pelo nome, para adicionar e/ou atualizar aplicações.

Trusted Users / Authorized Users: somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.

Trusted Time Window / Update Mode: janela de tempo para manutenção de aplicações.

Deve ser capaz de proteger em modo standalone - online ou offline;

Deve ser capaz de prevenir a criação de novos arquivos (incluindo diretórios e chaves de registro);

Deve ser capaz de monitorar a modificação de arquivos existentes, diretórios e chaves de registro;

Caso o arquivo seja sensível ou crítico, o administrador pode optar por receber um e-mail detalhando cada alteração realizada;

Deve ser capaz de limitar não apenas a escrita em chaves de registro, mas também a leitura;

A solução deve prover um conjunto de regras que limitam as ações nas chaves de registro;

Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do orgão;

Deve prevenir as seguintes ações:

Deletar;

Renomear;

Criar links;

Modificar Conteúdo;

Alterar o dono;

Deve ser capaz de monitorar alterações relacionadas as contas de usuários dentro dos seguintes parâmetros:

Criação de Conta

Alteração de Conta

Deleção de Conta

Log On (Sucesso e Falha)

Log Off

Deve suportar o monitoramento de atributos para os seguintes tipos de arquivo:

Zip;Tar;Dll;Exe;Jar;Sys;7z;Bz2;Bz;Tgz;Gz;Bmp;Jpg;tiff

Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento (Exemplo: %HOMEPATH%, % HOMEDRIVE%, %USERPROFILE%, %APPDATA%)

Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo: %PROGRAMFILES (x86)%)

Deve ser possível comparar dois arquivos ou duas versões de um arquivo da mesma estação de trabalho ou de estações diferentes, como forma de mitigar possíveis ameaças persistentes;

Deve ser possível autorizar usuários específicos que terão privilégios de alteração nos arquivos e chaves de registro protegidos na estação de trabalho;

Essa autorização deve utilizar o Active Directory para importar os usuários autorizados;

Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:

Critical Address Space Protection;

NX - No eXecute (mp-nx)

Virtual Address Space Randomization

Mp-vasr-rebase

Mp-vasr-randomization

Mp-vasr-relocation

Mp-vasr-reloc

Forced DLL Relocation

Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho.

Permitir o bloqueio de aplicações e os processos que a aplicação interage

Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não.

Permitir monitoração de Hooking de aplicações onde se podem determinar quais processos pode ser executado ou não

Proteção Adaptativa de Ameaças

O módulo de inteligência contra ameaças deve conter os seguintes mecanismos:

Confinamento dinâmico de aplicações:

A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware)

A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;

Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico

Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada

Solução deve manter um cache de reputação local com informações de aplicações – conhecidas, desconhecidas e maliciosas: Deve ser possível a classificação de cada aplicativo de maneira manual e até mesmo sua reclassificação através da console de administração central.

Dentre os comportamentos maliciosos, deve ser capaz de: Bloquear acesso local a partir de cookies; Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs; Criação de arquivos em qualquer local de rede; Criação de novos CLSIDs, APPIDs e TYPELIBs; Criação de threads em outro processo; Bloquear a desativação de executáveis críticos do sistema operacional; Leitura/Exclusão/Gravação de arquivos visados por Ransomwares; Gravação e Leitura na memória de outro processo; Bloqueio de Modificação da política de firewall do windows; Bloqueio de Modificação da pasta de tarefas do Windows; Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro; Bloqueio de Modificação de arquivos executáveis portáteis; Bloqueio de Modificação de bit de atributo oculto; Bloqueio de Modificação de bt de atributo somente leitura; Bloqueio de Modificação de entradas de registro de DLL AppInit; Bloqueio de Modificação de locais do registro de inicialização; Bloqueio de Modificação de pastas de dados de usuários; Bloqueio de Modificação do local do Registro de Serviços; Bloqueio de Suspensão de um processo; Bloqueio de Término de outro processo.

Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.

Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada.

O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário

A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção

Reputação local de ameaças

O módulo de reputação local deve manter uma base de dados com todos os executáveis detectados no ambiente.

Para cada executável, deverão ser apresentadas as reputações: Local; Centro de Inteligência do Fabricante; Analisador Dia Zero; Filtro de Conteúdo Web.

Deve permitir uma visualização analítica sobre cada arquivo detectado no ambiente, com no mínimo as seguintes informações: Data do último acesso; Tamanho do arquivo; Se está listado no Adicionar/Remover programas do Windows; Data de compilação; Registrado como serviço; Registrado como autorun; Mais de 6 meses de idade; Idade foi falsificada; Executado a partir do cmd.exe.

Deve ser capaz de informar a URL de origem do arquivo e sua reputação;

Deve permitir integração com base global de virus – VirusTotal – para comparação e se o arquivo sob análise já foi detectado por outro fabricante;

Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de “machine-learning”;

Deve ser capaz de user a técnica de “machine-learning” sem conectividade com a nuvem do fabricante.

Deve permitir o rastreamento da execução do arquivo malicioso pelo ambiente informando qual foi a sua primeira execução e sua última: Deve permitir a identificação da estação de trabalho e do usuário associado a mesma;

O módulo deve permitir automatização de contramedidas a partir de soluções do mesmo fabricante e de fabricantes terceiros;

Módulo Detecção, Resposta e Adaptação

A solução deve ser capaz de implantar o pilar de Detecção, Resposta e Adaptação.

Módulo de Detecção

Deve possuir painel único de visibilidade das ameaças do momento que se inicia, como se moveu pelo ambiente e toda a timeline da ameaça em questão.

Deve possuir capacidade automática de priorização de riscos baseado no comportamento da ameaça, permitindo uma investigação mais ágil do que é prioritário

Deve ser possível pesquisar informações da ameaça em tempo real e em modo histórico para determinar o escopo completo do ataque.

Deve permitir o monitoramento do ambiente através de coletores customizados para buscar por indicadores de ataques que não estão somente em execução, mas também por ameaças em modo dormente e demais que foram deletadas.

Módulo de Resposta

Deve ser capaz de utilizar gatilhos e reações para detectar eventos de ameaça e reagir de maneira automatica.

Deve ser capaz de implementar visibilidade dos dados gerados pelo Endpoint, através dos seguintes coletores: Processos; Flows de Rede; Arquivos; Perfil de Usuários; Registro do Windows; Updates Instalados; Grupos Locais Informação do Host.

Deve ser capaz de permitir a criação de coletores customizados para a coleta das informações desejadas;

Deve permitir a configuração de gatilhos que resultarão em uma reação ou contramedida frente ao dado coletado;

Deve ser capaz de implementar ações nos sistemas classificados como comprometidos;

Deve permitir a execução de scripts nas linguagens: Comandos do Sistema Operacional; PowerShell; Bash; Python; Visual Basic

Deve vir com políticas de monitoramento pré-configuradas pelo fabricante da solução;

Deve ser capaz de executar busca por padrões nas estações clientes em tempo real;

O campo de busca deve ser intuitivo e sugerir campos de informação durante a inserção de informações (autocompletar)

Deve ser capaz de salvar buscas realizadas previamente;

Deve ser capaz de apresentar, no mínimo, as seguintes informações após a busca: Endereço IP Local; Hash do processo em execução; ID do processo; Status da transação TCP; Número da porta que originou o pacote de rede; Nome do arquivo; Última data de gravação do arquivo; Data de Criação do arquivo; Data de deleção do arquivo; Versão do Sistema Operacional; Nome do Grupo de usuários; Se o grupo é local; SID do grupo; MAC de origem; MAC de destino; FLAGS TCP (ACK, SYN, RST e FIN); Número de transação TCP; Kernel Time; User Time; Comando que iniciou o processo; Quantidade de RAM utilizada pelo processo; Quantidade de Threads criadas pelo processo; MD5 do processo; SHA-1 do processo; Valor da chave de registro Caminho da chave de registro.

A resposta a uma determinada condição deverá ser executada como um serviço não interativo;

Deve permitir a execução de reação diretamente do painel de visibilidade de ameaças, permitindo por exemplo que se pare um processo malicioso em execução.

Módulo de Adaptação

Deve possuir a capacidade de criação de coletores e reações customizadas para melhor adaptar as investigações de ameaças e fluxos de detecção.

Deve possuir a capacidade de adaptar as configurações de proteção para bloquear ataques persistentes.

Ao registrar um artefato malicioso, esta predisposição (Malicioso ou Não Malicioso) deverá ser informada aos componentes interconectados.

Módulo de Análise Dia Zero

Caso o endpoint detecte um novo arquivo no ambiente, este deve ser encaminhado ao módulo dia zero para análise

Deve ser capaz de analisar os seguintes tipos de arquivos

Arquivos Executáveis (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl)

Arquivos Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf)

Arquivos Compactados (.zip, .rar)

Arquivos de Aplicativos Android (.apk)

Arquivos Java (jar)

Dispor de engine de múltiplas fases para verificação de Malwares e códigos maliciosos, dentre elas:

Deve se integrar com o centro de inteligência do fabricante para verificar se o arquivo já foi identificado em outro local do mundo

Deve possuir capacidade de emulação de arquivos

Deve possuir motor de análise contra malwares (antivirus engine)

Deve possuir capacidade de Desempacotar Malwares

Deve possuir capacidade de emulação de código

Deve possuir capacidade de Disassembly do código

Deve ser capaz de realizar Análise Dinâmica através de sandbox (instâncias de máquinas virtuais)

Deve realizar análise heurística (IE-FFx-Acrobat Emulation) baseado em análise estatística comportamental da geometria do arquivo, semântica e comportamento do código.

Deve realizar o Desempacotamento e análise do código latente

Deve realizar a análise estática de código e aplicar a engenharia reversa automatizada e o disassembly da análise de código

Deve permitir a análise de modo interativo durante a execução dinâmica do código

A análise dinâmica deve suportar a execução nos seguintes ambientes:

Android

Windows XP Service Pack 3

Windows 7 - 32 bits

Windows 7 - 64 bits

Windows Server 2003

Windows Server 2008 Service Pack 1

Windows Server 2008 R2

Deve suportar a análise de URL's submetidas para a solução

Deve ser capaz de inspecionar arquivos criptografados

Toda a verificação e análise de Malwares e/ou códigos maliciosos devem ocorrer em tempo real, não sendo aceitas verificações em cache engine ou batch mode

Analisar de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador

Deve possuir mecanismo para a identificação de Malwares em anexos de e-mails e URLs

Detectar Malwares que utilizem mecanismo de Exploit em arquivos, como PDF

Toda a verificação e análise de Malwares e/ou códigos maliciosos devem ocorrer em tempo real, não sendo aceitas verificações em cache engine ou batch mode

Módulo de Gerência

A gerência deve ser centralizada e suportar a gestão de todos os módulos listados neste Termo de Referência;

Não serão aceitas soluções que possuam mais de uma console de gestão;

Deve suportar a instalação nos seguintes sistemas operacionais:

Windows Server 2012 Release 2;

Windows Server 2012

Windows Server 2008 Service Pack 2 (SP2) Standard, Enterprise ou Datacenter;

Windows Server 2008 R2 Standard, Enterprise ou Datacenter;

A arquitetura dos Sistemas Operacionais deve ser 64-bits;

Deve suportar a instalação em Cluster Microsoft;

Deve suportar Ipv4 e Ipv6;

Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:

Vmware ESX

Microsoft Hyper-V

Deve possuir suporte a base de dados:

SQL Server 2012 ou superior

Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;

A console de gerência deve ser acessada via WEB;

Deve possuir compatibilidade com os seguintes browsers:

Google Chrome;

Firefox;

Internet Explorer 7 ou superior;

Safari 6.0 ou superior;

Deve ser possível segregar a instalação da solução em:

Servidor Console Central

Servidor Base de Dados

Servidor de Interação com os Agentes

Agentes Distribuidores de Vacina

Permitir a instalação dos Módulos da Solução a partir de um único servidor

Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota

Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE nesta contratação presente ou futura.

Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.

Visualização das características básicas de hardware das máquinas

Integração e Importação automática da estrutura de domínios do Active Directory já existentes na rede local

Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede.

Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado

Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.

Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados.

Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente

Permitir a criação de grupos virtuais através de “TAGs”

Permitir aplicar as “TAGs” nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;

Forçar a configuração determinada no servidor para os clientes;

Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente.

A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS

Forçar a instalação dos Módulos da Solução nos clientes;

Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido.

Customização dos relatórios gráficos gerados;

Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML

Geração de relatórios que contenham as seguintes informações:

Máquinas com a lista de definições de vírus desatualizada;

Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;

Os vírus que mais foram detectados;

As máquinas que mais sofreram infecções em um determinado período de tempo

Os usuários que mais sofreram infecções em um determinado período de tempo

Gerenciamento de todos os módulos da suíte;

Possuir dashboards no gerenciamento da solução;

Ao identificar um novo arquivo sendo executado, este deve ser submetido ou comparado a base do Virustotal;

Deve ser capaz de identificar e apresentar uma visibilidade sobre quais estações executaram um determinado arquivo (executável);

Deve ser capaz de identificar o arquivo e bloqueá-lo baseado na reputação e em critério de risco;

Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:

Cobertura da proteção de Navegação Segura;

Relatório dos últimos 30 dias da detecção de códigos maliciosos;

Top 10 Computadores com Infecções;

Top 10 Computadores com Sites bloqueados pela politica;

Resumo das ações tomadas nos últimos 30 dias no que se refere a Filtro de Navegação na web;

Resumo dos tipos de sites acessados nos últimos 30 dias no que se refere a Filtro de Navegação Segura;

Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota

Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva

Ter a capacidade de gerar registros/logs para auditoria

A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.

A solução de gerenciamento deve permitir acesso a sua console via web.

Especificação técnica do item 02 - Renovação das Licenças, Suporte e Manutenção de antivírus para desktops e servidores EDR (McAfee Endpoint Detection & Response)

Características Gerais da Solução

Deve possuir suporte a arquiteturas 32-bits e 64-bits;

Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 3Gb de memória RAM;

Deve suportar as seguintes plataformas clientes:

- Windows 10;
- Windows 8.1
- Windows 8;
- Windows 7;
- Sierra 10.12.x
- El Captain 10.11.x

Deve suportar as seguintes plataformas servidores:

- Windows Server 2016;
- Windows Server 2012 R2;
- Windows Server 2012;
- Windows Storage Server 2012;
- Windows 2008 R2 (Standard/Datacenter/Enterprise/Web)
- Deve inclusive suportar o modo Server Core;

Deve suportar, pelo menos a função de antivírus, as seguintes distribuições de Linux:

- Red Hat Enterprise 5.x e 6.x, 32 e/ou 64bits;
- Ubuntu 10.04, 11.04, 11.10, 12.04, 12.10, 13.04 e 13.10, 32 e/ou 64bits;
- CentOS 5.x e 6.x, 32 e/ou 64bits;

Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:

Microsoft Hyper-V 2012 R2;

Vmware ESXi;

Vmware Player;

Vmware vShpere;

Vmware Workstation;

Deve possuir proteção, pelo menos da funcionalidade de antivírus, para ambientes de Storage, incluindo:

IBM;

HP;

DELL;

Toda a proteção deverá ser realizada através de um único agente de proteção com as funcionalidades descritas neste termo, não sendo aceitos plugins ou softwares adicionais para a composição do pacote;

O agente único deve compreender as seguintes funcionalidades:

Prevenção de Ameaças

Firewall

Controle Web

Inteligência contra Ameaças

Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:

Relatórios;

Dashboards;

Políticas;

Configuração;

Instalação/Desinstalação;

O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente.

O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfix'es a partir de um servidor definido pelo administrador ou diretamente nos servidores da McAfee.

A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente;

A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;

A solução deve conter módulo capaz de proteger contra botnets, negação de serviço, executáveis não confiáveis e conexões web maliciosas;

A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)

A solução deve conter módulo capaz de garantir integração entre as soluções do fabricante proposto e entre fabricantes terceiros, compartilhando as informações do paciente dia zero para melhor mitigar novas ameaças.

Este módulo deve estar público para o desenvolvimento da comunidade via Github;

Proteção Clientes Windows - Proteção de Ameaças

Prevenção de exploração:

Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).

Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.

Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.

Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;

Deve ser possível incluir exclusões por:

Processo: Nome; Caminho do Arquivo; Hash MD5

Módulo chamador: Nome; Caminho; Hash MD5; Signatário Digital

Proteção de acesso

Deve fornecer regras de proteção nativamente, ou seja definida pelo fabricante da solução, no mínimo, para:

Acesso remoto a pastas locais; Alteração políticas de direitos dos usuários; Alterar os registros de extensão dos arquivos; Criação de novos arquivos na pasta Arquivo de Programas; Criação de novos executáveis na pasta Windows; Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema; Criar ou Modificar remotamente arquivos ou pastas; Desativar o editor de registro e o gerenciador de tarefas; Executar arquivos das pastas do usuário; Execução de scripts pelo host de script do Windows; Instalar objetos de ajuda a navegação ou extensões de shell; Instalar novos CLSIDs, APPIDs e TYPELIBs; Modificar configurações de rede; Modificar configurações do Internet Explorer; Modificar processos principais do Windows; Navegadores iniciando programas da pasta de downloads; Registrar programas para execução automática;

As regras especificadas devem permitir o seu:

Bloqueio, ou

Informação, ou

Bloqueio e Informação;

Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parametros:

Processos: Nome do processo; Hash MD5; Assinatura Digital;

Usuário

Arquivos: Criação;Deletar;Executar;Alteração de permissão;Leitura;Renomear;Escrever;

Chave de Registro: Escrever;Criar;Deletar;Ler;Enumerar;Carregar;Substituir;Restaurar;Alterar permissão;

Valor de Registro: Ler;Criar;Deletar;

Processo: Qualquer acesso;Criar thread;Modificar;Terminar;Executar;

Deve permitir a criação de exclusões;

Varredura ao acessar

A Varredura deve ser passível de habilitação/desativação por opção do administrador;

Deve iniciar a proteção durante a inicialização do sistema operacional;

Deve ser capaz de realizar análise no setor de boot;

O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;

Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo;

Deve possibilitar ao administrador a análise de instaladores confiáveis;

Deve realizar análise durante copia entre pastas locais;

A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;

Deve permitir a configuração do nível de agressividade da análise entre:

Muito Baixo

Baixo

Médio

Alto

Muito Alto

Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;

Deve realizar varredura quando o processo:

Ler o disco;

Gravar no disco;

Deixar a solução de proteção decidir;

Deve possibilitar análise em

Unidades de Rede;

Arquivos abertos para backup;

Arquivos compactados, por exemplo .jar;

Arquivos codificados (MIME)

Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;

Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

Limpar o arquivo;

Excluir o arquivo;

Negar acesso ao arquivo;

Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

Limpar o arquivo;

Excluir o arquivo;

Permitir acesso ao arquivo;

Negar acesso ao arquivo;

Deve possibilitar ao administrador a gestão de uma lista de exclusões;

Deve possuir módulo capaz de interceptar scripts destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;

Deve permitir a criação de listas de exclusão de URL's que não sofrerão interceptação e análise de scripts;

Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

Varredura sob demanda

Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.

Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.

Deve permitir a criação de repetição da tarefa.

Deve permitir definir a hora da execução da tarefa de análise;

Deve permitir a criação da tarefa de varredura de maneira aleatória;

Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.

Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:

Os locais da varredura, dentre eles: Memória para rootkits; Processos em execução; Arquivos registrados; Meu computador; Todas as unidades locais; Todas as unidades fixas; Todas as unidades removíveis; Todas as unidades mapeadas; Pasta inicial; Pasta de perfil do usuário; Pasta Windows; Pasta de arquivos de programas; Pasta temporária; Lixeira; Arquivo ou pasta especificada pelo administrador; Setor de inicialização (boot); Arquivos compactados; Arquivos MIME.

Os tipos de arquivos que serão analisados;

Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.

Áreas de exclusão que não deverão ser varridas;

Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada para a detecção de ameaças desconhecidas.

Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

Limpar o arquivo;

Excluir o arquivo;

Negar acesso ao arquivo;

Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

Limpar o arquivo;

Excluir o arquivo;

Permitir acesso ao arquivo;

Negar acesso ao arquivo;

Para minimizar o impacto ao usuário, a solução deve permitir:

Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;

Iniciar a varredura apenas quando o sistema estiver ocioso;

Permitir ao usuário retomar varreduras pausadas;

Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;

Proteção de Rede

O módulo de Firewall deve incluir as seguintes capacidades:

Deve permitir a ativação/desativação do módulo de Firewall através da console;

Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura contra ataques dia zero;

Deve possuir um firewall de estação statefull bloqueando tráfego de entrada e controlando o tráfego de saída;

Deve possuir assinaturas de proteção para:

Arquivos

Chave de Registro

Processos

Serviços;

Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;

Deve ser possível bloquear trafego bridge;

Deve ser possível bloquear contra falsificação de IP (IP Spoofing)

O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;

Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;

Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações:

Nome

Nome do arquivo ou Caminho;

Hash MD5

Assinador Digital

Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;

As conexões identificadas pelo Centro de Inteligência podem ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.

Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;

Deve permitir inspeção do protocolo FTP;

Deve ser possível bloquear trafego de protocolos não suportados;

O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.

O módulo de firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parametros:

Ação: Bloquear; Permitir

Direção: Ambas; Entrada; Saída

Protocolo: Qualquer protocolo; Protocolo IP (Ipv4;Ipv6; Protocolo Não-IP); Tipo de Conexão (Rede Sem Fio; Rede Cabeada; Rede Virtual); Especificação da Rede (Endereço IP; Subnet; Range; FQDN); Protocolo de Transporte (Todos; ICMP; ICMPv6; TCP; UDP; STP; GRE; IGMP; IPSEC AH; IPSEC ESP; Ipv6 in Ipv4; ISIS over Ipv4; L2TP); Agendamento (Dias da Semana; Hora Inicio; Hora Fim); Aplicações

Proteção Web

O modulo de Controle Web deve possuir as seguintes funcionalidades:

Deve permitir o bloqueio de browsers não suportados, dentre eles:

Opera

Safari for Windows;

Netscape

Maxthon

Flock;

Avant Browser;

Deepnet Explorer

PhaseOut

Deve permitir o controle de browsers suportados, dentre eles:

Chrome

Firefox

Internet Explorer

Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado.

Deve possuir, no mínimo, as seguintes categorias:

Browser Exploits; Download Maliciosos; Sites Maliciosos; Phishing; Pornografia; Hacking/Computer Crime; Spyware/Adware/Keyloggers; Anonymizer; Anonymizer Utilities; Alcohol; Blogs/Wiki; Business; Chat; Content Server; Dating; Dating/Social Networking; Digital Postcards; Discrimination; Drugs; Education; Entertainment; Extreme; Fashion; Finance; For Kids; Forum; Gambling; Game/Cartoon Violence; Games; General News; Government/Military; Gruesome Content; Health; Historical Revisionism; History; Humor/Comics; Illegal UK; Incidental Nudity; Information Security; Instant Messaging; Interactive Web Applications; Internet Radio/TV; Internet Services; Job Search; Major Global Religions; Marketing/Merchandising; Media Downloads; Media Sharing; Messaging; Mobile Phone; Moderated; Motor Vehicles; Non-Profit/Advocacy/NGO; Nudity; Online Shopping; P2P/File Sharing; Parked Domain; Personal Network Storage; Personal Pages; Pharmacy; Politics/Opinion; Portal Sites; Potential Criminal Activities; Potential Illegal Software; Potentially Unwanted Programs;Profanity; Professional Networking; Provocative Attire; Public Information; Real Estate; Recreation/Hobbies; Religion/Ideology; Remote Access; Residential IP Addresses; Resource Sharing; Restaurants; School Cheating Information; Search Engines; Sexual Materials; Shareware/Freeware; Social Networking; Software/Hardware; Spam URLs; Sports; Stock Trading; Streaming Media; Technical Information; Technical/Business Forums; Text Translators; Text/Spoken Only; Tobacco; Travel; Uncategorized; Usenet News; Violence; Visual Search Engine; Weapons; Web Ads; Web Mail; Web Meetings; Web Phone

Deve ser possível bloquear um site conforme a sua classificação:

Alto Risco

Médio Risco

Não categorizado

Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;

Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;

Deve permitir a varredura de arquivos baixados da internet;

Deve ser possível excluir endereços IP da análise;

Deve permitir a busca segura para buscadores, dentre eles:

Google;

Yahoo

Bing;

Ask;

Deve bloquear links que direcionem para sites com alto risco.

Deve permitir a customização das mensagens apresentadas para o usuário;

Caso o módulo detecte que exista um McAfee Web Gateway na rede, deverá deixar a análise a cargo deste último.

Proteção Adaptativa de Ameaças

O módulo de proteção contra ameaças deve conter os seguintes mecanismos:

Confinamento dinâmico de aplicações:

A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware)

A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;

Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico

Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada

Solução deve manter um cache de reputação local com informações de aplicações – conhecidas, desconhecidas e maliciosas: Deve ser possível a classificação de cada aplicativo de maneira manual e até mesmo sua reclassificação através da console de administração central.

Dentre os comportamentos maliciosos, deve ser capaz de: Bloquear acesso local a partir de cookies; Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs; Criação de arquivos em qualquer local de rede; Criação de novos CLSIDs, APPIDs e TYPELIBs; Criação de threads em outro processo; Bloquear a desativação de executáveis críticos do sistema operacional; Leitura/Exclusão/Gravação de arquivos visados por Ransomwares; Gravação e Leitura na memória de outro processo; Bloqueio de Modificação da política de firewall do windows; Bloqueio de Modificação da pasta de tarefas do Windows; Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro; Bloqueio de Modíficação de arquivos executáveis portáteis; Bloqueio de Modificação de bit de atributo oculto; Bloqueio de Modificação de bt de atributo somente leitura; Bloqueio de Modificação de entradas de registro de DLL AppInit; Bloqueio de Modificação de locais do registro de inicialização; Bloqueio de Modificação de pastas de dados de usuários; Bloqueio de Modificação do local do Registro de Serviços; Bloqueio de Suspensão de um processo; Bloqueio de Término de outro processo.

Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.

Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada.

O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;

A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção;

Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de “machine-learning”;

O módulo de inteligência contra ameaças deve conter os seguintes mecanismos:

Solução de Base de Dados Local de Ameaças

Da Arquitetura

A solução deve ser compreendida nos seguintes módulos:

Servidor de Orquestração e Base de Dados

Agentes

O servidor de orquestração deverá habilitar a troca de informação de ameaças entre os itens propostos neste edital, compreendendo:

Solução de Proteção de Endpoints

Solução para análise de malwares dia zero

A instalação do componente central deverá habilitar um protocolo de troca de informações de ameaças que permita o intercambio de informações entre soluções do mesmo fabricante e de fabricantes terceiros;

A troca de informação de ameaças deve ser dar por meio de protocolo performático;

O servidor de orquestração deve permitir a instalação em modo centralizado ou em modo descentralizado, permitindo que localidades remotas possuam um servidor local;

De forma a permitir menor impacto na rede, para tal o método de consulta dos clientes a base de dados poderá ser síncrona ou assíncrona;

Da solução

A solução deve possuir capacidade de criar uma reputação local através da catalogação de todos os executáveis existentes no ambiente;

A solução deverá apresentar a reputação definida para cada um dos ativos conectados, dentre eles:

Reputação Local

Reputação do Analisador de Malware dia Zero

Reputação do Filtro de Conteúdo Web

Reputação do Centro de Inteligência

A solução deve possuir capacidade de criar uma reputação local através da catalogação de todos os executáveis existentes no ambiente;

Ao catalogar um arquivo, a solução deve apresentar, no mínimo, as seguintes informações sobre o mesmo:

Nome do arquivo

Caminho do arquivo

Hash SHA-1

Hash MD5

Hash 256

Primeira visualização do arquivo na rede

Última visualização do arquivo na rede

Tamanho do arquivo

Data de compilação

Se o mesmo consta no Adicionar/Remover Programas

Se está registrado como serviço

Se está registrado para ser executado automaticamente

Tipo de compactador

Se é arquivo do sistema

Se foi executado a partir do cmd.exe

Se tem entrada no menu iniciar

Se foi executado a partir de uma mídia removível

Se foi executado a partir da raiz da unidade do sistema

Caso o arquivo tenha como origem a Internet, a solução deverá ser capaz de informar a partir de qual URL o arquivo foi obtido e a reputação desta última;

Deve ser possível realizar uma pesquisa do arquivo em base de conhecimento de terceiros (Exemplo: VirusTotal);

Após análise o administrador deve ter a possibilidade de:

Rastrear em quais estações o arquivo foi executado;

Identificar o país de origem do arquivo;

Identificar o arquivo como confiável;

Identificar o arquivo como desconhecido;

Identificar o arquivo como malicioso

Deve ser capaz de analisar o certificado associado ao arquivo;

Deve ser capaz de identificar o certificado associado como confiável ou malicioso;

Para minimizar o impacto a solução deve ter a capacidade de ser ativada no modo de observação;

Deve ser possível configurar o limiar mínimo para bloqueio de arquivos, variando entre:

Malicioso

Provavelmente malicioso;

Desconhecido

Deve ser possível bloquear a execução de arquivos nunca antes visto no ambiente e informar o usuário por meio de mensagem customizada em Português.

Caso a solução detecte arquivos não verificados pela solução de análise de dia zero, esta deverá ser capaz de enviar os arquivos de maneira automática para análise.

Deve ser capaz de identificar manualmente um arquivo como malicioso impedindo sua execução no ambiente;

Deve ser gerenciado pela mesma console proposta na Solução de Proteção de Endpoints.

Módulo de Proteção de Email

Servidores Microsoft Exchange Server

Compativeis com as plataformas Windows 2008 e Windows 2012

Suporte a exchange 2007 SP2 ou superior, Exchange 2010 SP2 ou superior e Exchange 2013

Rastreamento em tempo real, para arquivos anexados a mensagens do Exchange, antes de entregar a mensagem na caixa

postal do(s) destinatário(s), com as seguintes opções:

Limpar o arquivo infectado e entregá-lo limpo para o(s) destinatário(s);

Gravar o arquivo infectado na área de segurança (quarentena) e não entregá-lo para o(s) destinatário(s);

Gerar notificações e alertas e entregar o arquivo para o(s) destinatário(s)

Rastreamento manual às pastas do Exchange, com opção de limpeza.

Programação de rastreamentos automáticos do Exchange com as seguintes opções:

Escopo: Todas as pastas locais, ou pastas específicas

Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena)

Freqüência: Horária, diária, semanal, mensal

Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional

Gerar notificações de eventos de vírus através de mensagens do Exchange para quem enviou e quem recebeu a mensagem, e para um Administrador (usuário opcional)

Identificação de remetente e destinatário das mensagens

Permitir bloqueios baseados nos seguintes critérios:

Tipo de arquivo;

Nome do arquivo;

Tamanho do arquivo;

Permitir a instalação em ambientes em Cluster Microsoft

Capacidade de filtragem de conteúdo por categorias como: Sexo, Drogas, entre outros;

Módulo de Controle de Dispositivos

Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, Ipods, Dispositivos Bluetooth, DVDs, e CDS regraváveis;

Deve permitir a configuração dos dispositivos nos modos:

Bloqueio, ou;

Somente Leitura;

Deve classificar os dispositivos removíveis em 3 categorias:

Gerenciado;

Ingerenciável (Exemplo: Bateria de Notebooks);

Não Gerenciado;

Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:

Tipo de BUS;

Classe do Dispotivo (Device Class)

ID do fabricante (Vendor ID)

ID do produto (Product ID)

Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:

Tipo de BUS

Se o sistema de arquivo é passível de escrita;

Se o sitema de arquivo é somente leitura;

Tipo de Sistema de Arquivo

Nome do Sistema de Arquivo;

Número de Série do Sistema de Arquivo;

Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado a rede do orgão libera o uso de pen-drive);

Módulo de Controle de Aplicações

O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas, aplicar o controle de execução imposto pela política e realizar controle e auditoria sobre as alterações realizadas pelos usuários;

Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes.

Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão;

Ao detectar um executável, a solução deverá consultar o Centro de Inteligência do fabricante e esta deverá informar um nível de confidência (Bom, Mau ou Não Classificado);

Deve ser possível criar uma imagem base para a criação de uma política geral;

Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;

A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos;

Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:

Desabilitado: proteção desativada

Monitoramento: Monitora toda a atividade da Estação de Trabalho;

Atualização: a cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido;

Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA-1).

A solução deve suportar as seguintes modalidades de proteção:

Application Whitelisting: criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impadidas de serem executadas.

Application Blocking / Blacklisting: criação de uma lista de aplicações não autorizadas que não podem ser executadas.

Memory Protection: monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.

Solução deve suportar criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.

Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação do aplicativo ou arquivo.

Suportar os mecanismos:

Application Code Protection: permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, etc) possam ser executados. Além disso, permite proteção contra adulterações de programas em Whitelist (ex.: arquivos do programa) e, opcionalmente, chaves de registros contra modificações em disco.

Memory Protection: permite proteção contra ataques e exploração de vulnerabilidades para os programas em Whitelist.

Suporta criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de Whitelist, através de:

Binário: binário específico identificado através de seu nome ou de algorítmo de verificação SHA-1.

Trusted Publisher: fornecedor específico, assinado digitalmente por um certificado de segurança emitido, para este fornecedor, por uma Autoridade Certificadora (CA – Certificate Authority).

Trusted Installer: software instalado por um programa instalador específico, identificações por seu algorítmo de verificação, independentemente de sua origem.

Trusted Directories: pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.

Trusted Program / Authorized Updater: programas identificados pelo nome, para adicionar e/ou atualizar aplicações.

Trusted Users / Authorized Users: somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.

Trusted Time Window / Update Mode: janela de tempo para manutenção de aplicações.

Deve ser capaz de proteger em modo standalone – online ou offline;

Deve ser capaz de prevenir a criação de novos arquivos (incluindo diretórios e chaves de registro);

Deve ser capaz de monitorar a modificação de arquivos existentes, diretórios e chaves de registro;

Caso o arquivo seja sensível ou crítico, o administrador pode optar por receber um e-mail detalhando cada alteração realizada;

Deve ser capaz de limitar não apenas a escrita em chaves de registro, mas também a leitura;

A solução deve prover um conjunto de regras que limitam as ações nas chaves de registro;

Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do orgão;

Deve prevenir as seguintes ações:

- Deletar
- Renomear
- Criar links
- Modificar Conteúdo

Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento (Exemplo: %HOMEPATH%, % HOMEDRIVE%, %USERPROFILE%, %APPDATA%)

Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo: %PROGRAMFILES (x86)%

Deve ser possível comparar dois arquivos ou duas versões de um arquivo da mesma estação de trabalho ou de estações diferentes, como forma de mitigar possíveis ameaças persistentes;

Deve ser possível autorizar usuários específicos que terão privilégios de alteração nos arquivos e chaves de registro protegidos na estação de trabalho;

- Essa autorização deve utilizar o Active Directory para importar os usuários autorizados;

Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:

- Critical Address Space Protection;
- NX – No eXecute (mp-nx)
- Virtual Address Space Randomization (Mp-vasr-randomization, Mp-vasr-relocation, Mp-vasr-reloc)
- Forced DLL Relocation

Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho.

Permitir o bloqueio de aplicações e os processos que a aplicação interage

Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não.

Permitir monitoração de Hooking de aplicações onde se podem determinar quais processos pode ser executado ou não.

Módulo de Gerência

A gerência deve ser centralizada e suportar a gestão de todos os módulos listados neste Termo de Referência;

Não serão aceitas soluções que possuam mais de uma console de gestão;

Deve suportar a instalação nos seguintes sistemas operacionais:

- Windows Server 2012 Release 2;
- Windows Server 2012
- Windows Server 2008 Service Pack 2 (SP2) Standard, Enterprise ou Datacenter;
- Windows Server 2008 R2 Standard, Enterprise ou Datacenter;
- A arquitetura dos Sistemas Operacionais deve ser 64-bits;

Deve suportar a instalação em Cluster Microsoft;

Deve suportar Ipv4 e Ipv6;

Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:

- Vmware ESX
- Microsoft Hyper-V

Deve possuir suporte a base de dados:

- SQL Server 2012 ou superior

Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;

A console de gerência deve ser acessada via WEB;

Deve possuir compatibilidade com os seguintes browsers:

- Google Chrome;

Firefox;

Internet Explorer 7 ou superior;

Safari 6.0 ou superior;

Deve ser possível segregar a instalação da solução em:

Servidor Console Central

Servidor Base de Dados

Servidor de Interação com os Agentes

Agentes Distribuidores de Vacina

Permitir a instalação dos Módulos da Solução a partir de um único servidor

Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota

Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE nesta contratação presente ou futura.

Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.

Visualização das características básicas de hardware das máquinas

Integração e Importação automática da estrutura de domínios do Active Directory já existentes na rede local

Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede.

Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado

Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.

Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados.

Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente

Permitir a criação de grupos virtuais através de “TAGs”

Permitir aplicar as “TAGs” nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;

Forçar a configuração determinada no servidor para os clientes;

Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente.

A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS

Forçar a instalação dos Módulos da Solução nos clientes;

Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido.

Customização dos relatórios gráficos gerados;

Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML

Geração de relatórios que contenham as seguintes informações:

Máquinas com a lista de definições de vírus desatualizada;

Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;

Os vírus que mais foram detectados;

As máquinas que mais sofreram infecções em um determinado período de tempo

Os usuários que mais sofreram infecções em um determinado período de tempo

Gerenciamento de todos os módulos da suíte;

Possuir dashboards no gerenciamento da solução;

Ao identificar um novo arquivo sendo executado, este deve ser submetido ou comparado a base do Virustotal;

Deve ser capaz de identificar e apresentar uma visibilidade sobre quais estações executaram um determinado arquivo (executável);

Deve ser capaz de identificar o arquivo e bloqueá-lo baseado na reputação e em critério de risco;

Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:

Relatório dos últimos 30 dias da detecção de códigos maliciosos;

Top 10 Computadores com Infecções;

Top 10 Computadores com Sites bloqueados pela politica;

Resumo das ações tomadas nos últimos 30 dias no que se refere a Filtro de Navegação na web;

Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota

Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva

Ter a capacidade de gerar registros/logs para auditoria

A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.

A solução de gerenciamento deve permitir acesso a sua console via web.

MODELO DE EXECUÇÃO DO OBJETO

A execução do objeto seguirá a seguinte dinâmica:

O início da execução objeto seguirá a data de assinatura do Contrato.

Quando da assinatura do Contrato, todas as licenças de todos os recursos existentes na FUNDACENTRO deverão ser renovadas, o que implica em imediata nova implantação.

Essa nova implantação deverá ser concluída em até 60 dias após a assinatura do Contrato.

A prestação dos serviços poderá ser realizada remotamente, podendo, por necessidade explicitada da FUNDACENTRO a execução on-site dos serviços (podendo ocorrer de segunda a sexta das 08h às 19h) considerando a criticidade do mesmo.

Os serviços serão executados mediante solicitação prévia da FUNDACENTRO, seguindo o modelo de Ordem de Serviço segue no ANEXO A.

A contratada deverá responsabilizar-se integralmente pelo fiel cumprimento do objeto contratado, prestando todos os esclarecimentos que forem solicitados pelo CONTRATANTE cujas reclamações se obriga a atender.

A entrega dos produtos deverá ocorrer no prazo máximo de 30 (trinta) dias corridos, contados da data de assinatura do contrato.

A Contratada deverá fornecer a última versão disponível das licenças de uso dos softwares ofertados, observando as características, condições, quantidades e especificações constantes do Termo.

Juntamente com os produtos, a Contratada entregará ao Contratante a documentação técnica completa e atualizada dos softwares licenciados, contendo os manuais técnicos, certificados de garantia e autenticidade, guias de instalação, inicialização, operação, adequação, mensagens auxiliares para solução de problemas, diagnósticos, especificações e outros pertinentes, todos redigidos em português do Brasil e/ou inglês.

A documentação técnica a ser fornecida deverá conter no mínimo os módulos descritos a seguir:

Documentação das funcionalidades: Este documento conterá as características técnicas dos produtos e suas funções, procedimentos e parâmetros de configuração, tabelas, ilustrações, etc.

Documentação de instalação e operação: Este documento conterá informações quanto aos procedimentos de instalação e operação, comandos e testes aplicáveis, procedimentos de inicialização e de configuração e gerência de desempenho, de falhas e de segurança pertinentes.

Correrão por conta da Contratada as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos, bem como para os casos de manutenção.

O recebimento dos produtos não exclui a responsabilidade da Contratada pela qualidade dos produtos, ficando a mesma obrigada a substituir, às suas expensas, no todo ou em parte, os produtos da contratação, não excluindo ou reduzindo essa responsabilidade, à fiscalização ou ao acompanhamento exercido pelo Contratante.

Os técnicos especializados da Contratada deverão se reunir com a equipe do STIC para definir a estratégia de renovação das licenças.

A execução de todos os serviços será em data e horário a ser estipulado pelo STIC.

Na conclusão de execução dos serviços deverá ser apresentado um relatório com todos os procedimentos realizados, que será avaliado pelo Fiscal do Contrato.

Os profissionais que efetuarão a instalação, a configuração, implementação e o suporte técnico deverão ser certificados pelo fabricante McAfee nas licenças definidas neste T.R.

Todos os dados atuais sobre infraestrutura de rede e topologia da FUNDACENTRO deverão ser solicitados pela Contratada;

O desenho da solução, incluindo, no mínimo, topologia, configurações de rede, e os endereçamentos IP´s, deverá ser

elaborado pela Contratada em conjunto com a FUNDACENTRO;

Todo o planejamento das fases de instalação, customização, homologação e implantação em produção deverão ser realizados pela Contratada, sendo necessária a aprovação da FUNDACENTRO;

A Contratada deverá definir os representantes e os responsáveis por cada fase a ser executada;

O profissional indicado pela licitante que for contratada para gerenciar o projeto (preposto) será responsável pela elaboração e condução do cronograma dos trabalhos junto às equipes internas da FUNDACENTRO, observada a especificação das fases de instalação, customização, homologação e implantação da solução em produção;

Durante o período de instalação e customização da solução, os técnicos da Contratada deverão ser mantidos à disposição da FUNDACENTRO para o atendimento de dúvidas e correções.

MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO

Inspeções e Diligências

A CONTRATANTE se reserva o direito de, a qualquer tempo, realizar diligenciamento no ambiente físico da CONTRATADA ou solicitar quaisquer documentações complementares visando aferir se todas as obrigações de ordem técnica, pessoal qualificado, operacional ou administrativa, bem como se a manutenção das condições de habilitação está sendo cumpridas.

Papéis e responsabilidades

Gestor do Contrato: Servidor com função gerencial responsável pelo processo de gestão do contrato; Caberá ao Gestor do Contrato, dentre outras atribuições, convocar reunião inicial com a CONTRATADA; encaminhar as Ordens de Serviços; encaminhar a indicação de
sanção(es), quando cabível, e autorizar a emissão da Nota Fiscal.

Fiscal Requisitante do Contrato: Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área responsável por fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação.

Fiscal Técnico do Contrato: Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área responsável em fiscalizar tecnicamente o Contrato.

Fiscal Administrativo do Contrato: Servidor representante da Área Administrativa da FUNDACENTRO, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

Preposto da CONTRATADA: Será o responsável administrativo, com poderes de representante legal para tratar de todos os assuntos relacionados ao contrato, atuando à luz da Instrução Normativa nº 01/2019 da SGD/ME e suas revisões, e em atenção ao art. 68 da Lei nº. 8.666/93. Será atribuição sua gerir a execução do serviço, objeto do contrato, por parte da CONTRATADA, objetivando garantir a execução e entrega dos serviços dentro dos prazos estabelecidos e atendendo todos os requisitos especificados neste Termo de Referência; Gerir as solicitações de mudanças feitas pela CONTRATANTE, formalmente encaminhadas; Responder, perante a CONTRATANTE, pela execução das solicitações; Participar periodicamente, a critério do CONTRATANTE, de reuniões de acompanhamento das atividades referentes à prestação do serviço em execução. Não há obrigatoriedade do PREPOSTO disponível fisicamente nas dependências da FUNDACENTRO. Todavia, o PREPOSTO, obrigatoriamente, deverá estar disponível fisicamente nas dependências da FUNDACENTRO, quando solicitado, principalmente enquanto houver a execução da prestação de serviços por parte da CONTRATADA à CONTRATANTE.

Formas de acompanhamento do Contrato

A execução do contrato será acompanhada de forma presencial, por meio de inspeções contínuas e avaliação dos serviços, conforme metodologia de avaliação descrita neste TERMO DE REFERÊNCIA.

Para o acompanhamento e fiscalização do Contrato serão utilizadas as disposições contidas na IN nº 01/2019, da SGD/ME, e subsidiariamente as disposições contidas na IN SLTI/MPOG nº 05/2017.

A execução técnica dos serviços deverá estar aderente às melhores práticas definidas pelo fabricante dos produtos, às boas práticas consagradas para atividades de TIC (especialmente àquelas específicas para questões de vulnerabilidades, cibersegurança e antivírus), além de estar aderente às diretrizes, normas e procedimentos definidos pelo STIC. A adequada execução técnica dos trabalhos será acompanhada pelo STIC a seu critério, que eventualmente poderá realizar procedimentos de inspeção.

Procedimentos e critérios de mensuração de prestação de serviços:

Níveis Mínimos de Serviço Exigidos (NMSE):

Indicador de Suporte Técnico (IST)	
Item	**Descrição**
Finalidade	Mede a qualidade do atendimento aos chamados de suporte técnico.
Meta a cumprir	Atender as demandas solicitadas durante a vigência contratual, nos prazos estabelecidos neste índice.
Método de medição	Por evento de chamado de suporte técnico realizado.

Forma de acompanhamento	Acompanhamento do fiscal do contrato ou representante técnico por ele indicado durante a execução do chamado técnico até o seu encerramento.
Periodicidade	Por evento
Tempo máximo para início de atendimento crítico - TMA	Até 4 (quatro) horas contadas a partir da abertura do chamado técnico na contratada (o STIC registrará o número do chamado e o horário de abertura)
Tempo máximo para início de atendimento moderado - TMA	Até 16 (dezesseis) horas contadas a partir da abertura do chamado técnico na contratada (o STIC registrará o número do chamado e o horário de abertura)
Tempo máximo para início de atendimento leve - TMA	Até 48 (quarenta e oito) horas contadas a partir da abertura do chamado técnico na contratada (o STIC registrará o número do chamado e o horário de abertura)
Sanções	Sanção 1 - TMA cumprido dentro do estipulado neste índice, não há incidência de advertência/multa. Sanção 2 – TMA com atraso até 8 (oito) horas do estipulado neste índice, aplicação de advertência de acordo com os termos deste TR e dos termos contratuais. Sanção 3 – TMA com atraso superior a 48 (quarenta e oito) horas do estipulado neste índice, aplicação de multa de acordo com a gradação da mesma, observando os termos deste TR e dos termos contratuais.
Observações	- Os atrasos deverão ser informados no relatório descritivo do serviço realizado no chamado técnico.

Condições de aceite

O aceite se dará de forma provisória (por meio de Termo de Recebimento Provisório - TRP) e definitiva (Termo de Recebimento Definitivo - TRD), conforme etapas e prazos descritos na subseção "DO RECEBIMENTO E ACEITAÇÃO DO OBJETO" a seguir.

Os trabalhos poderão ser acompanhados e auditados por profissionais da CONTRATANTE, que se certificarão do atendimento dos objetivos definidos e a conformidade com as normas e melhores práticas pertinentes.

O recebimento provisório ou definitivo não exclui a responsabilidade pelas atividades técnicas executadas, nem a responsabilidade ético-profissional pela perfeita execução do Contrato, dentro dos limites estabelecidos em Lei.

À CONTRATADA caberá sanar as irregularidades apontadas na execução contratual, submetendo a uma nova verificação as entregas ou atividades impugnadas, ficando sobrestado o pagamento da ordem de serviço correspondente até o saneamento necessário, sem
prejuízo da aplicação das sanções legais cabíveis.

OBRIGAÇÕES DA CONTRATANTE

Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017.

Não praticar atos de ingerência na administração da Contratada, tais como:

exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

Considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada;

Arquivar, entre outros documentos, projetos, "as built", especificações técnicas, orçamentos, termos de recebimento,

contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas;

Fiscalizar o cumprimento dos requisitos legais, quando a contratada houver se beneficiado da preferência estabelecida pelo art. 3º, § 5º, da Lei nº 8.666, de 1993.

OBRIGAÇÕES DA CONTRATADA

Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017;
Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;

Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato.

Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.

Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo.

Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a contratada houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015.

Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

Assegurar à CONTRATANTE, em conformidade com o previsto no subitem 6.1, “a”e “b”, do Anexo VII – F da Instrução Normativa SEGES/MP nº 5, de 25/05/2017:

O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à Contratante distribuir, alterar e utilizar os mesmos sem limitações;

Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da Contratante, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

DA SUBCONTRATAÇÃO

Não será admitida a subcontratação do objeto licitatório.

ALTERAÇÃO SUBJETIVA

É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993.

O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 87 da Lei nº 8.666, de 1993.

As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

A fiscalização técnica dos contratos avaliará constantemente a execução do objeto e utilizará o disposto no item 7 deste TR para aferição da qualidade da prestação dos serviços, podendo a Contratata incorrer nas penalides ali descritas, sempre que (e considerando que) a Contratada:

> não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
>
> deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

A utilização do disposto no item 7 não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação

dos serviços.

Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à CONTRATADA de acordo com as regras previstas no ato convocatório.

O fiscal técnico poderá realizar avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da CONTRATADA que contenha sua relação detalhada, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

As disposições previstas nesta cláusula não excluem o disposto no Anexo VIII da Instrução Normativa SLTI/MP nº 05, de 2017, aplicável no que for pertinente à contratação.

A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos abaixo.

No prazo de até 5 dias corridos do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual;

O recebimento provisório será realizado pelo fiscal técnico após a entrega da documentação acima, da seguinte forma:

A contratante realizará inspeção minuciosa de todos os serviços executados, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários.

Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato

A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

A Contratante emitirá Termo de Recebimento Provisório (conforme modelo no Anexo II) referente aos produtos entregues pela CONTRATADA.

No prazo de até 10 dias corridos a partir do recebimento dos documentos da CONTRATADA, cada fiscal ou a equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao gestor do contrato.

Quando a fiscalização for exercida por um único servidor, o relatório circunstanciado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do último.

> Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

No prazo de até 10 (dez) dias corridos a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

Emitir Termo Circunstanciado para efeito de recebimento definitivo dos bens e serviços prestados (conforme modelo no Anexo II), com base nos relatórios e documentações apresentadas; e

Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor.

Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

DO PAGAMENTO

O pagamento será efetuado pela Contratante no prazo de 10 (dez) dias, contados do recebimento da Nota Fiscal/Fatura.

Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme este Termo de Referência

A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

o prazo de validade;

a data da emissão;

os dados do contrato e do órgão contratante;

o período de prestação dos serviços;

o valor a pagar; e

eventual destaque do valor de retenções tributárias cabíveis.

Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

não produziu os resultados acordados;

deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.
Nota Explicativa: Para que seja possível efetuar a glosa, é necessário definir, objetivamente, no IMR ou instrumento equivalente, quais os parâmetros para mensuração do percentual do pagamento devido em razão dos níveis esperados de qualidade da prestação do serviço.

Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	$I = \frac{(6 / 100)}{365}$	I = 0,00016438 TX = Percentual da taxa anual = 6%

REAJUSTE

Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o Índice de Custos de Tecnologia da Informação - ICTI, conforme a Portaria nº 6.432, de 11 de julho de 2018, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

O reajuste será realizado por apostilamento.

GARANTIA DA EXECUÇÃO

O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% (cinco por cento) do valor total do contrato.

No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contados da assinatura do contrato, a contratada deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou

títulos da dívida pública, seguro-garantia ou fiança bancária.

A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017.

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

prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

multas moratórias e punitivas aplicadas pela Administração à contratada; e

obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

Será considerada extinta a garantia:

com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

A contratada autoriza a contratante a reter, a qualquer tempo, a garantia, na forma prevista no neste Edital e no Contrato.

DAS SANÇÕES ADMINISTRATIVAS

Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

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

ensejar o retardamento da execução do objeto;

falhar ou fraudar na execução do contrato;

comportar-se de modo inidôneo; ou

cometer fraude fiscal.

Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

Multa de:

0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na

execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo; e

0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

as penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos

A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 19.1 deste Termo de Referência.

Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

As sanções previstas nos subitens 17.2.1, 17.2.3, 17.2.4 e 17.2.5 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas dos itens 17.5 e 17.6:

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor mensal do contrato
2	0,4% ao dia sobre o valor mensal do contrato
3	0,8% ao dia sobre o valor mensal do contrato
4	1,6% ao dia sobre o valor mensal do contrato
5	3,2% ao dia sobre o valor mensal do contrato

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou conseqüências letais, por ocorrência;	05
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento;	04
3	Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia;	03
4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	02
5	Retirar funcionários ou encarregados do serviço durante o expediente, sem a anuência prévia do CONTRATANTE, por empregado e por dia;	03
Para os itens a seguir, deixar de:		
6	Registrar e controlar, diariamente, a assiduidade e a pontualidade de seu pessoal, por funcionário e por dia;	01
7	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	02
8	Substituir empregado que se conduza de modo inconveniente ou não atenda às necessidades do serviço, por funcionário e por dia;	01
9	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência;	03
10	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato;	01
11	Providenciar treinamento para seus funcionários conforme previsto na relação de obrigações da CONTRATADA	01

Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

As penalidades serão obrigatoriamente registradas no SICAF.

CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.

Os critérios de qualificação econômica a serem atendidos pelo fornecedor estão previstos no edital.

Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão:

Organização da Proposta:

Prazo de validade não inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

Preço considerando o período de 24 (vinte e quatro) meses, de acordo com os preços praticados no mercado, conforme estabelece o art. 43, inciso IV, da Lei nº 8.666/93, em algarismo e por extenso, expresso em moeda corrente nacional (R$), considerando as especificações constantes no Termo de Referência.

Estar incluídos no preço todos os insumos que o compõe, tais como as despesas com mão de obra, impostos, taxas, frete, seguros e quaisquer outros que incidam direta ou indiretamente no fornecimento dos programas objeto desta licitação.

A proposta deverá conter a especificação clara e completa da solução ofertada e prestação dos serviços, obedecida a mesma ordem constante do termo de referência relacionado, sem conter alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado.

A licitante deverá manter profissionais necessários a execução dos serviços de suporte, com o perfil e qualificações mínimas exigidas a seguir, mantendo o compromisso de atualizá-los e capacitá-los sempre que houver atualização tecnológica nos softwares fornecidos:

Profissional certificado em solução McAfee que compreenda tanto os recursos do Complete Endpoint Protection Business (CEB) quanto do Endpoint Detection & Response (EDR).

Qualificação Técnica da Contratada (apresentação obrigatória)

Para fins de comprovação da qualificação técnica, é necessário apresentar o atestado indicados a seguir:

Atestado de Capacitação Técnica, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, comprovando ter fornecido, para organizações públicas ou privadas, fornecimento de softwares antivírus McAfee, bem como serviços de suporte nesse software.

A LICITANTE poderá apresentar mais de um atestado para fim de composição e comprovação da qualificação técnica. Os atestados devem possibilitar determinar de forma inequívoca o período de execução dos serviços.

No conteúdo dos atestados deve constar expressamente o serviço que foi executado pelo licitante, a sua “execução a

contento" e o item específico a ser comprovado.

Os atestados para comprovação da aptidão para desempenho de atividade pertinente e compatível (ou superior) em características e volume ao demandado pela FUNDACENTRO deverão ser emitidos, em documento timbrado, pela pessoa jurídica de direito público ou privado com a qual esta mantém (manteve) contrato de prestação de serviços, e deverá conter o nome, cargo ou função, dados de identificação (CPF e identidade), telefone e e-mail de contato do(s) seu(s) emissor(es), que possibilitem à FUNDACENTRO, por intermédio de seu Pregoeiro, caso julgue necessário, confirmar sua veracidade junto ao cedente emissor.

A FUNDACENTRO reserva-se no direito de executar diligências para verificar e validar as informações prestadas no(s) atestado(s) de capacidade técnica fornecido(s) pelo vencedor do certame. Também poderão ser requeridos cópia do(s) contrato(s), nota(s) fiscal(is) ou qualquer outro documento que comprove, inequivocamente, a veracidade do(s) atestado(s).

O documento apresentado pela licitante para comprovação de sua qualificação técnica, além de possuir informações técnicas e operacionais suficientes para qualificar o escopo realizado, deverá conter dados que possibilitem à FUNDACENTRO, por intermédio de seu Pregoeiro, caso julgue necessário, confirmar sua veracidade junto ao cedente emissor, como por exemplo: número e período de vigência do contrato, especificação do serviço executado, nome, cargo e telefone institucional para contato junto ao emitente.

No caso de atestados emitidos por empresas privadas, não serão aceitos aqueles emitidos por empresas do mesmo grupo empresarial da empresa proponente.

Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

O critério de julgamento da proposta é o menor preço global.

As regras de desempate entre propostas são as discriminadas no edital.

ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS

O valor global máximo a ser admitido pela FUNDACENTRO para a presente contratação é de R$ 133.648,00, o qual corresponde ao custo total da renovação das licenças de software antivírus por 24 (vinte e quatro) meses de vigência do Contrato, conforme tabela a seguir:

Item	Descrição do Item (Objeto)	CATMAT/CATSER	Quantidade	Unidade de Medida	Valor (R$)	
					Unitário	Total
1	Renovação de Licença de Software Unificado de Gerenciamento de Antivírus CEB (Complete Endpoint Protection Business)	350949	400	unidade	194,27	77.708,00
2	Renovação das Licenças, Suporte e Manutenção de antivírus para desktops e servidores EDR (McAfee Endpoint Detection & Response)	350949	400	unidade	139,85	55.940,00
					Global	133.648,00

DOS RECURSOS ORÇAMENTÁRIOS

As despesas decorrentes com a referida aquisição correrão à conta da Dotação Orçamentária da União, conforme detalhado abaixo. Fonte de Recursos:

Programa/Ação: 100, 250 ou 280 (2110/2000)

Natureza da Despesa: 339039

ANEXOS

ANEXO I - Modelo de Planilha de Custos e Formação de Preços

ANEXO II - Modelo de Ordem de Serviço de Manutenção e Suporte Técnico

ANEXO II - Modelo de Termo de Recebimento Provisório

ANEXO III - Modelo de Termo de Recebimento Definitivo

O presente documento segue assinado pelo servidor Elaborador, pela autoridade Requisitante e pela autoridade responsável pela Aprovação da conveniência e oportunidade, com fulcro no art. 9º, inciso II, do Decreto nº 5.450/2005 e art. 15 da IN nº 02/2008-SLTI/MPOG, cujos fundamentos passam a integrar a presente decisão por força do art. 50, § 1º, da Lei nº

9.784/1999.

ANEXO I - MODELO DE PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS

ID	Descrição	Qtd	Vlr. Unitário	Vlr. Total
1	Renovação de Licença de Software Unificado de Gerenciamento de Antivírus CEB (Complete Endpoint Protection Business)	400		
2	Renovação das Licenças, Suporte e Manutenção de antivírus para desktops e servidores EDR (McAfee Endpoint Detection & Response)	400		
Valor por extenso				

ANEXO II - MODELO DE ORDEM DE SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

FINALIDADE:	***<objeto do serviço>***

DADOS DA ORDEM DE SERVIÇO	
Contrato:	***<número do contrato>***
Objeto e descrição detalhada da O.S.: <...>	
DETALHES DA ORDEM DE SERVIÇO	
Data de atendimento <presencial/remoto>: <data>	
Fiscal do Contrato: <nome do fiscal do contrato>	

Atendimento da O.S.		
Data e hora do início do atendimento:		**Data e hora do término do atendimento:**
<data/hora> _____ _____:_____		<data/hora> _____ _____:_____
Observações: _____ _____ _____ _____ _____		

DE ACORDO	
CONTRATANTE **Fiscal Técnico do Contrato**	**CONTRATADA** **Preposto**
_____ <nome do fiscal técnico do contrato> Matr.: <nº da matrícula>	_____ <nome do preposto> CPF: <nº do CPF do preposto>

Local, <dia> de <mês> de <ano>	Local, <dia> de <mês> de <ano>

ANEXO III - MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

INTRODUÇÃO				
O Termo de Recebimento Provisório declara formalmente à Contratada que os serviços foram prestados ou os bens foram recebidos para posterior análise das conformidades de qualidade, baseadas nos critérios de aceitação definidos em contrato.				
IDENTIFICAÇÃO				
Contrato nº: [XXXXXXX] Contratada: [XXXXXX] Contratante: [XXXXXX]				
Ordem de Serviço / Ordem de Fornecimento de bem Nº: <OS9999/AAAA>	Data da Emissão: <dia> de <mês> de <ano>.			
Bem/Solução de TI				
ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES DE EXECUÇÃO				
Item	Descrição de Produto e Serviço	Unidade	Quantidade	Total
1.	<Descrição>			
...				
TOTAL DE ITENS				

Por este instrumento, atestamos para fins de cumprimento do disposto na Instrução Normativa nº 01, de 04 de abril de 2019-SGD/ME, que os bens, relacionados na OS/OFB acima identificada, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo CONTRATANTE. Ressaltamos que o recebimento definitivo destes bens ocorrerá em até XXXX dias úteis, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

DE ACORDO	
CONTRATANTE **Fiscal Técnico do Contrato**	**CONTRATADA** **Preposto**
_____ <nome do fiscal técnico do contrato> Matr.: <nº da matrícula> Local, <dia> de <mês> de <ano>	_____ <nome do preposto> CPF: <nº do CPF do preposto> Local, <dia> de <mês> de <ano>

ANEXO IV - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO	
O Termo de Recebimento Definitivo declarará formalmente a Contratada que os serviços prestados ou os bens fornecidos foram devidamente avaliados e atendem aos requisitos estabelecidos em contrato.	
IDENTIFICAÇÃO	
Contrato nº [XXXXXXX] Contratada: [XXXXXX] Contratante: [XXXXXX]	
Ordem de Serviço (O.S.) Nº: <XXXXXXXX>	Data da Emissão: <dia> **de** <mês> **de** <ano>.
Solução de TI	

ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES DE EXECUÇÃO				
Item	Descrição de Produto e Serviço	Métrica	Quantidade	Total
1.	<Descrição igual da OS de abertura>	<PF ou outra>		
...				
TOTAL DOS ITENS				

Por este instrumento, atestamos para fins de cumprimento do disposto na Instrução Normativa nº 01, de 04 de abril de 2019-SGD/ME, que os bens integrantes da **O.S.** acima identificada, ou conforme definido no contrato supracitado, atendem às exigências especificadas no Termo de Referência do Contrato acima referenciado.

DE ACORDO	
Gestor do Contrato	**Fiscal Requisitante do Contrato**
_____ <nome do gestor do contrato> Matr.: <nº da matrícula> Local, <dia> de <mês> de <ano>.	_____ <nome do fiscal requisitante do contrato> <Qualificação> Local, <dia> de <mês> de <ano>.

Documento assinado eletronicamente por **Diego Ricardi dos Anjos**, **Chefe de Serviço**, em 02/04/2020, às 10:34, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Fabio Akio Shiomi Iha**, **Chefe de Serviço**, em 02/04/2020, às 10:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Tatiana Goncalves**, **Chefe de Serviço**, em 02/04/2020, às 10:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Norisvaldo Ferraz Junior**, **Analista em C&T**, em 02/04/2020, às 10:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marina Brito Battilani**, **Diretora**, em 03/04/2020, às 16:56, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Felipe Memolo Portela**, **Presidente**, em 08/04/2020, às 16:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.fundacentro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0046770** e o código CRC **55F7EB52**.

Referência: Processo nº 47648.000293/2020-35 SEI nº 0046770

Criado por norisjunior, versão 86 por diego.anjos em 01/04/2020 15:45:12.