JUSTIÇA FEDERAL
Tribunal Regional Federal da 1ª Região

PREGÃO ELETRÔNICO SRP Nº 24/2022

PAe/SEI nº: 0013621-23.2021.4.01.8000

Órgão Gerenciador TRF1 - Código UASG: 090027

Órgãos Participantes:

SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG - Código UASG: 090013

FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS - Código UASG: 154419

O **TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO**, por intermédio da Pregoeira designada pela Portaria Diges n. 282, de 22 de julho de 2022, torna pública a abertura de procedimento licitatório na modalidade Pregão, **do tipo menor preço, PELO SISTEMA DE REGISTRO DE PREÇOS, modo de disputa ABERTO E FECHADO,** a ser realizado por meio de tecnologia da informação, obedecidos aos preceitos da Lei 10.520, de 17 de julho de 2002, do Decreto 7.174, de 12 de maio de 2010, do Decreto 10.024, de 20 de setembro de 2019, do Decreto 7.892, de 23 de janeiro de 2013, da Lei Complementar 123, de 14 de dezembro de 2006, do Decreto 8.538, de 6 de outubro de 2015, aplicando-se subsidiariamente as disposições da Lei nº 8.666, de 21 de junho de 1993 e subordinando-se às condições e exigências estabelecidas neste Edital.

1 - DO OBJETO

1.1 - A presente licitação tem por objeto a formação de registro de preços para eventual contratação de empresa especializada no fornecimento, desinstalação, instalação e configuração de licenciamento de solução de antivírus, com garantia e atualização de versões, pelo período de 60 (sessenta) meses, bem como serviços de suporte especializado e treinamento, para as estações de trabalho e equipamentos servidores da Justiça Federal da 1ª Região (Órgão Gerenciador) e Órgãos Participantes, conforme quantidades, especificações e localidades, constantes deste Edital e seus Anexos.

1.2 - Observe-se que **as especificações contidas no Edital SEMPRE prevalecerão em relação àquelas contidas no código BR,** do Portal de Compras do Governo Federal.

2 - DA ABERTURA DA SESSÃO PÚBLICA

Data: 12/09/2022

Horário: 14:00 horas (horário de Brasília)

Local: **https://www.gov.br/compras/pt-br/**

3 - DAS CONDIÇÕES DE PARTICIPAÇÃO

3.1 - Poderão participar deste Pregão Eletrônico os interessados que atenderem a todas as exigências, inclusive quanto à documentação, constantes deste Edital e seus anexos, e que estiverem devidamente credenciados no site: **https://www.gov.br/compras/pt-br/**.

3.2 - O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico.

3.3 - O credenciamento junto ao Portal de Compras do Governo Federal implica a responsabilidade legal da licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

3.4 - O uso da senha de acesso ao sistema eletrônico é de inteira e exclusiva responsabilidade da licitante, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao Tribunal Regional Federal da Primeira Região responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

3.5 - A licitante deverá manifestar, em campo próprio:

a) o cumprimento dos requisitos para a habilitação e a conformidade de sua proposta com as exigências deste edital;

b) que inexistem fatos impeditivos para sua habilitação;

c) que não emprega menor;

d) que atende aos requisitos do art. 3º da LC nº 123/2006, com alterações, para fazer jus aos benefícios previstos nessa lei, quando for o caso;

e) que atende aos requisitos previstos na legislação, caso seja apta ao exercício do direito de preferência estabelecido no Decreto n.º 7.174/2010**;**

f) que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, nos termos do art. 93 da Lei nº 8.213/91, quando for o caso;

g) que cumpre a cota de aprendizagem nos termos estabelecidos no art. 429 da CLT, quando for o caso;

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

3.5.1 – A falsidade da declaração de que trata a letra "a" sujeitará a licitante às sanções previstas neste Edital.

3.6 - Não será permitida a participação de empresas:

a) que estejam sob pena de interdição de direitos previstos **na Lei nº 9.605, de 12.02.98 (Lei de Crimes Ambientais);**

b) reunidas em consórcio ou que sejam controladoras, coligadas ou subsidiárias entre si;

c) que se encontrem sob falência, concurso de credores ou em processo de dissolução ou liquidação;

c.1. Na hipótese de empresas em recuperação judicial ou extrajudicial, a participação dependerá de comprovação, respectivamente, da concessão ou da homologação do plano de recuperação pelo juízo competente, bem como do atendimento aos requisitos de qualificação econômico-financeiro previstos neste edital.

d) suspensas de participar em licitação e impedidas de contratar com o **Tribunal Regional Federal da 1ª Região ou com os Órgãos Participantes**, nos termos do art. 87, inciso III, da Lei 8.666/1993;

e) impedidas de licitar e contratar com a União, nos termos do art. 7º da Lei nº 10.520/02;

f) declaradas inidôneas para licitar e contratar com a Administração Pública nos termos do art. 87, inciso IV da Lei 8.666/93.

g) proibidas de contratar com o Poder Público, em decorrência de condenação definitiva com fundamento *art. 12, d*a Lei 8.429/1992 (consulta ao banco de dados do CNJ: Cadastro Nacional de Condenados por Ato de Improbidade Administrativa e por Ato que Implique Inelegibilidade – CNCIAI);

h) suspensas ou que tenham interdição parcial de suas atividades, nos termos do art. 19 da Lei 12.846/2013 (Lei Anticorrupção), evidenciada em consulta ao banco de dados do *Cadastro Nacional de Empresas Punidas (CNEP).*

3.7 - Incluem-se na vedação estabelecida no subitem anterior, as hipóteses previstas no art. 9º da Lei 8.666/93.

4 - DO ENVIO DAS PROPOSTAS

4.1 - A licitante interessada em participar do Certame **deverá encaminhar,**

concomitantemente com os documentos de habilitação exigidos no item 9 deste Edital, **sua proposta com a descrição do objeto ofertado, marca, modelo e o preço unitário cada item**, com apenas duas casas decimais, exclusivamente por meio eletrônico, no site https://www.gov.br/compras/pt-br/, a partir da data da liberação do edital no Portal de Compras do Governo Federal, até a data e hora de abertura da sessão pública.

4.2 – Na formulação da proposta, as licitantes devem observar as seguintes condições:

a) redigir sua oferta em português, sem emendas, rasuras, cotações alternativas ou entrelinhas, constar nome do Representante Legal e o número do seu registro no Cadastro Nacional de Pessoas Jurídicas;

b) indicar de modo claro e inequívoco o número deste Pregão, o dia e hora da realização da Sessão Pública, bem como os seguintes dados da licitante: endereço, e-mail, telefone e nome do representante legal da empresa, responsável pela assinatura do Contrato/Ata de Registro de Preços;

c) descrever individualmente e com clareza a identificação da solução ofertada, as quantidades, os valores e outras informações aplicáveis, obedecidas as especificações contidas neste Edital e seus Anexos;

d) consignar os preços unitários, mensais, totais e total proposto para o grupo, conforme modelo de Planilha para Formulação de Preços, constante do Anexo II deste Edital, adequando-os ao último lance ofertado ou valor negociado. Observe-se que **os lances deverão ser ofertados pelo valor unitário proposto para cada item**, com no máximo duas casas decimais;

e) prever o **prazo de entrega, na última versão do software, por meio de chaves de acesso ao site do fabricante,** que não poderá ser superior **10 (dez) dias úteis**, contados a partir do recebimento da Ordem de Fornecimento;

f) indicar o **prazo de execução dos serviços de desinstalação, instalação e configuração,** que não poderá ser superior **44 (quarenta e quatro) dias úteis,** contados do aceite provisório dos itens 1, 2, 5 e 6 (licenças);

g) estabelecer o **prazo de início do serviço de treinamento,** que não poderá ser superior **a 10 (dez) dias úteis**, contados do recebimento da ordem de execução de serviço, bem como, o **prazo de execução dos serviços de treinamento,** que não poderá ser superior a **10 (dez) dias úteis**, contados a partir do seu início;

h) fixar **prazo de garantia e atualização** das licenças**,** não inferior a **60 (sessenta) meses,** contados a partir da data de assinatura do Termo de Recebimento Definitivo;

i) apresentar**, juntamente com a proposta, declaração:**

i.1) de acordo com a condição da empresa**, que não está sob pena de interdição de direitos previstos na Lei nº 9.605, de 12.02.98** (Lei de Crimes Ambientais);

i.2) que ateste que a empresa **não pratica registro de oportunidade** junto ao fabricante;

j) informar o **prazo de validade da proposta,** que **não** poderá ser **inferior a 60 (sessenta) dias**, contado do dia útil imediatamente posterior ao indicado no item 02 deste Edital;

k) encaminhar, juntamente com a proposta, para os itens 01, 02, 05 e 06**:**

k.1) manuais, catálogos, folhetos, impressos ou publicações originais do fabricante ou outros documentos suficientes para comprovação dos requisitos técnicos do software ofertado(tais como cópia de tela), fazendo constar da proposta técnica a identificação e página do documento onde se encontra descrita cada uma das características ofertadas. Caso a licitante não disponha destes documentos, deverá apresentar declaração do fabricante em questão com as referidas especificações;

k.2) Formulário de Avaliação Técnica, conforme Anexo III;

l) incluir nos preços ofertados todos os custos decorrentes da contratação, tais como: transporte, mão de obra, impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, embalagens, prêmios de seguro, fretes, taxas e outras despesas incidentes ou necessárias à efetivação dos fornecimentos na forma prevista neste Edital.

4.3 - Será permitido o uso de expressões técnicas de uso comum na língua inglesa.

4.4 - A licitante deverá apresentar proposta considerando a última versão de software disponível pelo fabricante, na data da licitação.

4.5 – A participação no certame, com a apresentação da proposta, concomitantemente com os documentos de habilitação, implicará plena aceitação, por parte da licitante, das condições estabelecidas neste edital e em seus anexos, não se lhe reconhecendo o direito à arguição de omissões, enganos ou erros posteriores que encerrem a pretensão de alterar o valor ofertado.

4.6 – Até a abertura da sessão, as licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

4.7 – Em nenhuma hipótese poderão ser alteradas as condições de pagamento, prazos ou outras que contrariem este Edital, salvo no que tange aos preços ofertados, que poderão ser reduzidos no curso da fase de lances do certame.

4.8 – Encerrada a etapa de lances e concluída a negociação, a licitante classificada provisoriamente em primeiro lugar **deverá encaminhar, no prazo**

máximo de 02 (duas) horas, exclusivamente via sistema eletrônico, em formato digital, no Portal de Compras do Governo Federal, por meio da opção “Enviar Anexo”, a proposta de preços ajustada ao valor do lance ou da negociação, **bem como documentos complementares reputados necessários, mercê de eventuais particularidades reconhecidas pela Pregoeira**.

4.9 – A pedido da licitante, via chat e justificadamente, o prazo concedido para envio do anexo a que se refere o subitem 4.8 poderá ser prorrogado pela Pregoeira, levando-se em conta o interesse deste Tribunal, a justificativa e a razoabilidade do pleito.

4.10 – A licitante que **deixar de enviar** a proposta indicada no subitem 4.8, no prazo estipulado, sem que tenha apresentado justificativa aceita pela Pregoeira, nos termos do subitem anterior, **terá sua proposta recusada e sujeitar-se-á à aplicação de penalidade**, na forma do subitem 13.4 deste Edital.

4.11 – Durante a análise da aceitação, na hipótese de serem detectados erros ou falhas sanáveis nas propostas ou nos documentos de habilitação apresentados, a Pregoeira poderá determinar à licitante vencedora respectivos ajustes, nos termos do art. 47 do Decreto 10.024/2019.

5 - DA ABERTURA DA SESSÃO PÚBLICA

5.1 - A Pregoeira e sua equipe de apoio obedecerão, na execução dos seus trabalhos, aos trâmites e procedimentos estabelecidos nos subitens abaixo.

5.1.1 – No horário estabelecido no item 2 deste edital, a Pregoeira efetuará a abertura das propostas encaminhadas pelo sistema “PREGÃO ELETRÔNICO”, por meio do site https://www.gov.br/compras/pt-br/.

5.1.2 – Classificadas as propostas, as licitantes poderão ofertar lances sucessivos, observado o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.

DA COMPETITIVIDADE (FORMULAÇÃO DE LANCES – MODO ABERTO E FECHADO)

6.1 – Aberta a etapa competitiva (sessão pública), as licitantes poderão ofertar lances públicos e sucessivos, com lance final e fechado, exclusivamente por meio do sistema eletrônico.

6.2 – Os lances deverão ser formulados pelo **VALOR UNITÁRIO proposto para cada ITEM.**

6.3 - Os lances oferecidos pela licitante deverão ser inferiores ao último por ela ofertado e registrado pelo sistema.

6.4 - A licitante poderá ofertar lances iguais ou superiores aos de outras

proponentes (lance intermediário, definido no inciso V do art. 3º do Decreto 10.024/2019), desde que estes sejam inferiores ao último lance ofertado por ela própria.

6.5 – No modo de disputa aberto e fechado, a oferta de lances terá a duração de 15 (quinze) minutos. Encerrado esse prazo, o sistema encaminhará o aviso de fechamento iminente dos lances. A partir desse marco, transcorrerá período aleatoriamente determinado de até dez minutos, que finalizará, automática e peremptoriamente, a recepção de lances.

6.6 – Encerrado o prazo de que trata o subitem 6.5, o sistema abrirá a oportunidade para que a licitante da oferta de valor mais baixo e as proponentes com valores até dez por cento superiores àquela possam ofertar um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento desse prazo.

6.7 – Na ausência de, no mínimo, três ofertas nas condições de que trata o subitem 6.6, as licitantes detentoras dos menores lances subsequentes, na ordem de classificação, até o máximo de três, poderão oferecer um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento desse prazo.

6.8 – Na ausência de lance final e fechado classificado nos termos dos subitens 6.6 e 6.7, haverá o reinício da etapa fechada, para que as demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até cinco minutos, que será sigiloso até o encerramento desse prazo.

6.9 – Na hipótese de não haver licitante classificado na etapa de lance fechado que atenda às exigências para habilitação, a Pregoeira poderá, motivadamente, admitir o reinício da etapa fechada, nos termos do disposto no subitem 6.8.

6.10 – Encerrados os prazos estabelecidos nos subitens 6.6 a 6.8, o sistema ordenará os lances em ordem crescente de vantajosidade.

6.11 – Após o início da fase competitiva, caso não haja envio de lances e havendo propostas com o mesmo valor, serão aplicados os critérios de desempate do artigo 36 do Decreto 10.024/2019, e subsistindo o empate, o sistema eletrônico elegerá a proposta vencedora por meio de sorteio, dentre as propostas empatadas.

6.12 – Durante o transcurso da sessão pública, a Pregoeira poderá enviar mensagens, via chat, às licitantes, que só poderão se comunicar com a Pregoeira por iniciativa desta, após o encerramento da fase de lances.

6.13 – No caso de desconexão, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível às licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

6.14 – Se a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente decorridas vinte e quatro horas após a comunicação expressa da Pregoeira aos

participantes, no endereço eletrônico utilizado para divulgação.

6.15 – É vedada a desistência de proposta ou de lances efetuados, sujeitando-se a proponente desistente às penalidades previstas no art. 49 do Decreto 10.024/2019.

7 — DOS CRITÉRIOS DE PREFERÊNCIA E DE DESEMPATE

7.1 – Encerrada a fase de lances, o sistema identificará a existência de Microempresas e Empresas de Pequeno Porte - ME/EPPs no Certame e fará uma comparação entre os valores por elas ofertados e o da primeira colocada, caso esta não seja ME/EPP.

7.2 – Será considerado empate quando uma ou mais ME/EPPs apresentarem propostas com valores iguais ou até 5% (cinco por cento) superiores à proposta mais bem classificada, ocasião em que a(s) ME/EPP(s) terá(ão) a preferência do desempate na ordem de classificação.

7.3 – A ME/EPP mais bem classificada, na faixa dos 5% da proposta de menor preço, terá o direito de, no prazo de 5 (cinco) minutos controlados pelo Sistema, encaminhar uma última oferta, obrigatoriamente abaixo da primeira colocada para o desempate, sob pena de decair do direito concedido.

7.4 – Na hipótese do subitem 7.3, caso a ME/EPP convocada desista ou não se manifeste no prazo estabelecido, o Sistema convocará as demais ME/EPPs participantes na mesma condição, na ordem de classificação.

7.5 – Não havendo ME/EPP ou quando não for exercido o direito previsto no subitem 7.3, e após a aplicação do critério estabelecido no § 2º do art. 3º da Lei 8.666/1993, em se tratando de fornecimento de bens e serviços de informática e automação, o Sistema assegurará o direito de preferência, na forma do art. 3º da Lei 8.248/1991 e Decreto 7.174/2010, obedecido o procedimento descrito nos subitens 7.6 e 7.7 deste instrumento.

7.6 – Serão convocadas, as licitantes, na ordem classificatória, cujas propostas finais estejam situadas em até 10% (dez por cento) acima da melhor proposta válida, com vistas ao exercício do direito de preferência, desde que atendam aos seguintes critérios:

I - bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal.

II - bens e serviços com tecnologia desenvolvida no País; e

III - bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal.

7.7 – Os fornecedores dos bens e serviços de informática e automação que declararem beneficiários do direito, nos termos da alínea "e" do subitem 3.5, deverão apresentar, juntamente com a proposta, sob as penas da lei, comprovação de que atendem aos requisitos estabelecidos no subitem 7.6.

7.8 – Caso nenhuma empresa classificada venha a exercer o direito de preferência, observar-se-ão as regras usuais de classificação e julgamento previstas na Lei 10.520/2002 e Decreto 10.024/2019.

8 — DA AVALIAÇÃO DE PROPOSTA E DE HABILITAÇÃO APÓS FASE DE LANCES

8.1 – Superada a fase de lances, a Pregoeira procederá ao exame de proposta e de habilitação.

8.2 – Após negociação, por meio do sistema eletrônico, **com a licitante autora da melhor proposta,** nas mesmas condições previstas em edital, e não se obtendo preço compatível com o valor estimado para a contratação, a Pregoeira recusará a proposta e direcionará contraproposta à licitante imediatamente classificada, e assim sucessivamente, até a obtenção do preço julgado aceitável;

8.3 – Obtida uma proposta de preços julgada aceitável e concluída a fase competitiva, a Pregoeira consultará a base de dados do SICAF para verificar o preenchimento dos requisitos habilitatórios fixados neste Edital;

8.4 – Constatado o desatendimento, pela licitante, de qualquer dos requisitos de habilitação, a Pregoeira examinará a aceitabilidade da proposta e o preenchimento das exigências habilitatórias por parte das remanescentes, até a apuração de uma proposta que atenda aos termos deste Edital.

8.5 – Encerrada a fase de habilitação e, não havendo quem pretenda recorrer, a Pregoeira adjudicará o objeto em favor da licitante julgada vencedora.

8.6 – Manifestando, qualquer das licitantes, a intenção de recorrer, e caso esta seja aceita, o processo somente será encaminhado para adjudicação e homologação do resultado após o transcurso da fase recursal.

8.7 – No ato da homologação, o sistema convocará as licitantes remanescentes, que poderão reduzir seus preços ao valor da proposta da licitante vencedora, para formação do cadastro reserva. A apresentação de novas propostas não prejudicará o resultado do certame em relação à licitante mais bem classificada (art. 10, caput e parágrafo único, art. 11, caput, inciso I e §1º do Decreto 7.892/2013).

8.8 – Caso entenda necessário examinar, mais detidamente, a conformidade das propostas com os requisitos estabelecidos neste edital, bem como, o preenchimento das exigências habilitatórias, poderá a Pregoeira suspender a

sessão, hipótese em que comunicará às licitantes, a data e o horário de reabertura da sessão pública.

8.9 - A Pregoeira e a autoridade superior do Tribunal Regional Federal da Primeira Região poderão pedir esclarecimentos e promover diligências destinadas a elucidar ou a complementar a instrução do processo, em qualquer fase da licitação e sempre que julgarem necessário, fixando às licitantes prazos para atendimento, sendo vedada a inclusão posterior de informação que deveria constar originariamente da proposta.

9 - DA HABILITAÇÃO

9.1 - Para habilitar-se na presente licitação, a licitante deverá incluir **concomitantemente com a proposta, até a data e o horário estabelecidos para a abertura da Sessão Pública**, exclusivamente por meio eletrônico, no Portal de Compras do Governo Federal, os documentos que não estejam contemplados no SICAF, conforme segue:

a) Documentação de Habilitação Jurídica;

b) Documentação de Qualificação Econômico-Financeira; e

c) Documentação de Regularidade Fiscal.

9.2 - A **habilitação jurídica** será comprovada mediante a apresentação da seguinte documentação:

9.2.1 - Ato constitutivo, estatuto ou contrato social, com a última alteração, devidamente registrado no órgão competente ou registro comercial, no caso de empresa individual;

9.2.1.1 – Em quaisquer dos atos constitutivos, deverá estar contemplada, dentre os objetivos sociais, a execução de atividades da mesma natureza ou compatíveis com o objeto da licitação.

9.2.2 - Caso o Representante Legal não esteja contemplado para tal no Contrato Social ou Estatuto da Empresa, deverá apresentar procuração.

9.2.2.1 – São aplicáveis as regras do art. 3º da Lei 13.726/2018 relativamente à autenticação de documentos.

9.2.3 - Decreto de autorização, no caso de empresa ou sociedade estrangeira em funcionamento no País.

9.3 – A qualificação Econômico-Financeira será comprovada mediante a apresentação da seguinte documentação**:**

9.3.1 - Certidão negativa de feitos sobre falência, expedida pelo distribuidor da sede da licitante, para atendimento da alínea "c" do subitem 3.6 este Edital;

9.3.2 - Balanço patrimonial e demonstrações contábeis referentes ao último exercício social, comprovando índices de Liquidez Geral - LG, Liquidez Corrente - LC, e Solvência Geral - SG superiores a 1 (um);

9.3.3 – A licitante que apresentar resultado igual ou menor que 1, em quaisquer dos índices - Liquidez Geral – LG, Solvência Geral – SG, e Liquidez Corrente – LC, deverá possuir Patrimônio Líquido mínimo de R$ 526.251,63 (quinhentos e vinte e seis mil, duzentos e cinqüenta e um reais e sessenta e três centavos) correspondente a 10% do valor estimado de um grupo da contratação, na forma da lei, vedada a substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrados há mais de 3 (três) meses da data da apresentação das propostas.

9.3.4 – Apresentar Capital Circulante Líquido ou Capital de Giro (Ativo Circulante - Passivo Circulante) de, no mínimo, R$ 526.251,63 (quinhentos e vinte e seis mil, duzentos e cinqüenta e um reais e sessenta e três centavos) equivalente a 10% do valor estimado de um grupo da contratação, tendo por base o balanço patrimonial e as demonstrações contábeis do último exercício social.

9.3.5 - As demonstrações contábeis deverão apresentar as assinaturas do titular ou representante da empresa e do contabilista responsável, legalmente habilitado.

9.3.6 - As demonstrações contábeis das empresas com menos de um exercício social de existência devem cumprir a exigência contida na lei, mediante a apresentação do Balanço de Abertura ou do último Balanço Patrimonial levantado.

9.4 - A **regularidade Fiscal e Trabalhista** será comprovada mediante consulta, da Pregoeira, ao Sistema de Cadastro Unificado de Fornecedores – SICAF, para verificação da validade dos documentos abaixo:

9.4.1 - prova de regularidade do Fundo de Garantia por Tempo de Serviço - FGTS, junto à Caixa Econômica Federal;

9.4.2 - prova de regularidade relativa à Seguridade Social, à Dívida Ativa da União e à Secretaria da Receita Federal, emitida pela Procuradoria Geral da Fazenda Nacional e/ou Receita Federal do Brasil;

9.4.3 - prova de regularidade para com a Fazenda Estadual da sede da licitante;

9.4.4 - prova de regularidade para com a Fazenda Municipal da sede da licitante, quando se tratar de empresa sediada fora do Distrito Federal;

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

9.5 - Havendo irregularidade no cadastramento ou habilitação parcial no SICAF, será assegurado à licitante, o direito de encaminhar a documentação atualizada constante dos subitens 9.3, 9.4.1 a 9.4.4, por meio da opção “Enviar Anexo” do Portal de Compras do Governo Federal**,** no prazo estipulado pela Pregoeira.

9.5.1 - Caso a validade dos documentos citados nos subitens 9.3, 9.4.1 a 9.4.4 esteja vencida no SICAF, poderá também, a Pregoeira, consultar sítios oficiais de

órgãos e entidades emissores das certidões, para verificar as condições de habilitação das licitantes.

9.6 – Havendo alguma restrição na comprovação de regularidade fiscal, **para as Microempresas e Empresas de Pequeno Porte,** será obedecido o prazo constante do art. 43 § 1º da Lei Complementar 123/2006 e art. 4º, § 1º do Decreto 8.538/2015.

9.7 - Além da documentação descrita nos subitens anteriores, a Pregoeira irá verificar a existência de registros impeditivos da contratação (Acórdão 1.793/2011 – Plenário-TCU), no Cadastro Nacional de Empresas Inidôneas e Suspensas/CGU (CEIS); e Cadastro Nacional de Empresas Punidas (CNEP) disponíveis no Portal da Transparência, no Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa, disponível no Portal do CNJ, e consultará a Certidão Negativa de Débitos Trabalhistas – CNDT, criada pela Lei 12.440, de 07/07/2011, prevalecendo a certidão mais recente sobre a mais antiga.

9.7.1 – Havendo alguma restrição relativa aos registros da empresa, será facultado à licitante, o envio de documento que comprove que a situação já foi regularizada.

9.7.2 - A Pregoeira verificará ainda, nos Portais da Transparência do Governo Federal e do Poder Judiciário, se o somatório de ordens bancárias recebidas pela licitante classificada, provisoriamente, em primeiro lugar, relativas ao último exercício ou ao exercício corrente, até o mês anterior ao da data desta licitação, fixada neste Edital, já seria suficiente para extrapolar o faturamento máximo permitido como condição para o benefício do tratamento jurídico diferenciado, previsto na Lei Complementar n.º 123/2006.

9.8 - Sempre que julgar necessário, a Pregoeira poderá solicitar a apresentação do original dos documentos apresentados pela licitante, não sendo aceitos “protocolos de entrega” ou “solicitações de documentos” em substituição aos comprovantes exigidos no presente Edital.

10 - DO JULGAMENTO

10.1 - O julgamento e a adjudicação do objeto desta licitação serão realizados pelo **VALOR TOTAL proposto para o GRUPO**.

10.2 - No julgamento desta licitação, levar-se-á em conta o valor ofertado pelas licitantes, devendo ser declarada vencedora aquela que, habilitada, seja também a autora do menor preço julgado aceitável pela Pregoeira, considerados os preços ofertados para os itens do grupo.

10.3 - Serão desclassificadas/recusadas as propostas:

a) com preços excessivos, para itens do grupo, ou manifestamente inexequíveis ou com valores totais ou unitários simbólicos, irrisórios ou iguais a zero;

b) que **não indicarem marca** ou **mencionarem mais de uma marca** para o mesmo item;

c) que não atendam às exigências técnicas obrigatórias;

d) elaboradas em desacordo com os termos deste Edital e seus Anexos, observado o disposto no art. 47 do Decreto 10.024/2019;

e) não anexadas nos termos do subitem 4.8 do Edital.

10.4 - Serão **inabilitadas** as empresas:

a) que não anexarem a documentação de habilitação, conforme estabelecido nos subitens 4.1 e 9.1 do Edital;

b) com impedimentos ou irregularidades, nos termos do subitem 9.8 deste Instrumento.

10.4.1 - A proponente que fizer indevida declaração de enquadramento como microempresa ou empresa de pequeno porte ou ao direito de preferência, constante do art. 5º do Decreto 7174/2010, será inabilitada e sujeitar-se-á às penalidades previstas neste instrumento.

11 - DA ATA DE REGISTRO DE PREÇOS

11.1 - A Ata de Registro de Preços terá validade de 12 (doze) meses, a contar da data de sua assinatura.

11.2 - O TRF 1ª Região e órgãos participantes não tem definição imediata de aquisição para as quantidades registradas, considerando que os pedidos ocorrerão mediante demanda da Unidade Requisitante.

11.3 - O TRIBUNAL REGIONAL DA 1ª REGIÃO – TRF1 é o Órgão Gerenciador e a SEÇÃO JUDICIÁRIA DE MINAS GERAIS e FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS são órgãos participantes desta ARP.

11.3 - Homologado o resultado da licitação e disponibilizada a Ata de Registro de preços no Sistema Eletrônico de Informações (SEI), a licitante vencedora, observado o disposto no art. 11 do Decreto 7.892/13, **deverá assiná-la eletronicamente, no prazo de 05 (cinco) dias úteis**, contados da data do envio da notificação, que será expedida para o e-mail indicado na proposta de preços, nos termos da alínea “b”, subitem 4.2 do Edital, sob pena de decair do direito a ter o seu preço registrado**.**

11.4 - O prazo fixado no subitem anterior poderá ser prorrogado uma única vez e por igual período, desde que a solicitação seja apresentada ainda durante o transcurso do interstício inicial, desde que ocorra motivo justificado e aceito pelo Tribunal Regional Federal da Primeira Região.

11.5 - É facultado à Administração, quando o convocado não assinar o referido documento no prazo e condições estabelecidas no subitem 11.4 deste Edital,

chamar as licitantes remanescentes, mesmo que não disponha de cadastro reserva obedecida a ordem de classificação, para assinatura da Ata de Registros de Preços, após comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e feita a negociação, podendo ainda, revogar a licitação, independentemente da cominação prevista no art. 49 do Decreto 10.024/2019.

11.6 - Não serão admitidas adesões à ARP, nos termos do Acórdão 1297/2015 TCU-Plenário.

11.7 - Informações da Ata serão disponibilizadas no Portal de Compras do Governo Federal e no sítio do Tribunal – http://portal.trf1.jus.br/portaltrf1/transparencia/licitacoes-e-compras/compras.htm.

11.8 - O extrato da Ata de Registro de Preços será divulgado em órgão oficial da Administração.

11.9 - Os preços registrados poderão ser revistos, obedecidas às disposições contidas nos arts. 17 e 18 do Decreto 7.892/2013 e 65, alínea "d", inciso II, da lei 8.666/1993.

11.10 - O fornecedor terá seu registro cancelado quando:

a) descumprir as condições da Ata de Registro de Preços;

b) não retirar a respectiva nota de empenho ou instrumento equivalente, no prazo estabelecido pela Administração, sem justificativa aceitável;

c) não aceitar reduzir o seu preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;

d) sofrer sanção prevista nos incisos III ou IV do caput do art. 87 da Lei 8.666/93, ou no art. 7º da Lei 10.520/02; e

e) tiver presentes razões de interesse público.

11.11 - O fornecedor poderá solicitar o cancelamento do seu registro de preço na ocorrência de fato superveniente que venha comprometer a perfeita execução contratual, decorrente de caso fortuito ou de força maior devidamente comprovado.

11.12 - Será realizada pesquisa de preços para comprovação da vantajosidade da contratação, conforme o disposto no inciso XI art. 9º do Decreto nº 7.892/13, quando decorridos 04(quatro) meses da homologação da licitação ou da data da última aquisição.

11.13- A figuração do licitante no cadastro reserva não obriga a administração à contratação.

12 – DA CONTRATAÇÃO

12.1 - Será firmado contrato com a licitante vencedora, o qual tomará por base os dispositivos da Lei nº 8.666/93, as condições estabelecidas neste Edital e seus anexos, bem como, as constantes da proposta apresentada pela adjudicatária.

12.2 - Após regular convocação por parte do Tribunal Regional Federal da Primeira Região ou Órgão Participante, a empresa adjudicatária terá prazo máximo de 05 (cinco) dias úteis para assinar o contrato, sob pena de, não o fazendo, decair do direito à contratação e/ou sujeitar-se às penalidades previstas neste Edital.

12.3 - O prazo fixado no subitem anterior poderá ser prorrogado uma única vez e por igual período, desde que a solicitação respectiva seja apresentada ainda durante o transcurso do interstício inicial, bem como que ocorra motivo justo e aceito pelo Tribunal Regional Federal da Primeira Região ou Órgão Participante.

12.4 - É facultado à Administração, quando o convocado não assinar o referido documento no prazo e condições estabelecidas, chamar as licitantes remanescentes, obedecida a ordem de classificação, para assinatura do Contrato, após comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e feita a negociação, podendo ainda, revogar a licitação, independentemente da cominação prevista no art. 49 do Decreto 10.024/2019.

12.5 - Será exigida da licitante vencedora, prestação de garantia correspondente a 5% (cinco por cento) do valor do contrato, numa das seguintes modalidades, conforme opção da Contratada:

a) caução em dinheiro ou títulos da dívida pública, devendo estes ser 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;

b) seguro-garantia;

c) fiança bancária.

12.6 - No caso da prestação de garantia na modalidade de caução em dinheiro, a Contratada deverá efetuar o depósito na Caixa Econômica Federal – CEF, Agência n. 2301 – PAB – Tribunal Regional Federal da Primeira Região, apresentando, logo em seguida, o comprovante ao Contratante.

12.7 - Em caso de apresentação de fiança bancária, na carta de fiança, deverá constar expressa renúncia, pelo fiador, aos benefícios do artigo 827 do Código Civil Brasileiro (Lei n. 10.406/2002).

12.7.1 – No instrumento de garantia, deve estar assegurado, expressamente, que o garantidor tem ciência das respectivas cláusulas de sancionamento e que, em caso de penalidade imposta pelo contratante, basta a apresentação da decisão

final exarada no processo administrativo, para que o correspondente valor seja recolhido em favor do erário, na forma fixada pela Administração, independentemente de anuência, autorização ou manifestação da Contratada.

12.8 - A apresentação do comprovante da garantia prestada deverá ser feita no prazo determinado pelo Contrato.

12.9 - As formas de pagamento, recebimento, obrigações das partes, penalidades contratuais e demais condições estabelecidas para o ajuste estão discriminadas na Minuta de Contrato, parte integrante deste Edital.

13 - DAS SANÇÕES ADMINISTRATIVAS

13.1 - Em caso de descumprimento das obrigações previstas neste instrumento, poderão ser aplicadas as seguintes sanções:

a) advertência;

b) multa;

c) impedimento de licitar e contratar com a União pelo prazo de até cinco anos (art. 7º da Lei 10.520/2002, c/c o art. 49 do Decreto 10.024/2019).

13.2 - As sanções previstas nas alíneas “a” e “c” do subitem 13.1 poderão ser aplicadas juntamente com a da alínea “b” do mesmo subitem.

13.3 – O **atraso injustificado** na devolução da Ata de Registro de Preços ou do Contrato assinado **sujeitará a licitante à multa diária de 0,1% (um décimo por cento)** calculado sobre o valor total da proposta, até o limite de 2% (dois por cento).

13.4 – Caso a empresa vencedora, sem motivo justificado, não anexar a documentação exigida no Certame, não mantiver a proposta ou causar atraso na execução do objeto, nos termos do subitem 4.10 deste edital, ser-lhe-á aplicada a sanção de impedimento de licitar e contratar com a União, prevista no subitem 13.1, alínea “c”.

13.4.1 - A recusa da licitante vencedora em assinar a Ata de registro de preços ou o Contrato caracterizará descumprimento total da obrigação, o que ensejará incidência de multa de 10% sobre o valor total de sua proposta, sem prejuízo da sanção prevista no subitem 13.1, alínea “c”.

13.5 - À licitante que cometer fraude fiscal, apresentar documento falso, fizer declaração falsa ou comportar-se de modo inidôneo será aplicada a pena prevista na alínea “c” do subitem 13.1, e será descredenciada no SICAF.

13.6 – As multas devidas ao Tribunal Regional Federal da 1ª Região ou Órgão Participante pela licitante serão recolhidas por meio de GRU em favor do Contratante, no prazo de 05 (cinco) dias úteis, contados do recebimento da notificação, ou cobrados judicialmente.

13.7 – As penalidades previstas neste edital, precedidas de regular processo administrativo, assegurados o contraditório e a ampla defesa, serão registradas no SICAF.

14 - DOS RECURSOS E DAS IMPUGNAÇÕES

14.1 - Declarada a vencedora, qualquer licitante poderá, durante a Sessão Pública, de forma imediata e motivada, em campo próprio do sistema, manifestar intenção de recorrer, quando lhe será concedido o prazo de 03 (três) dias para apresentar as razões do recurso, ficando as demais licitantes, desde logo, intimadas para, querendo, apresentarem contrarrazões em igual prazo, que começará a correr após o término do prazo da recorrente. Observe-se que **os recursos deverão ser formalizados, exclusivamente, por meio eletrônico**, em campo próprio disponibilizado pelo Portal de Compras do Governo Federal.

14.2 - A falta de manifestação imediata e motivada da licitante quanto à intenção de recorrer, nos termos do subitem anterior, importará na decadência desse direito. A não apresentação das razões do recurso no prazo legal caracterizará desistência do recurso.

14.3 - Os recursos contra anulação ou revogação da licitação, rescisão do contrato, bem como contra a aplicação das penas de advertência, suspensão temporária ou de multa, poderão ser interpostos no prazo máximo de 05 (cinco) dias úteis, contados da data em que se verificar a intimação dos interessados.

14.4 - Qualquer pessoa que pretender impugnar os termos deste Edital deverá fazê-lo por meio de expediente escrito dirigido à Pregoeira, exclusivamente na forma eletrônica, para o e-mail dilit@trf1.jus.br, observada a antecedência mínima de 03 (três) dias úteis, contados da data fixada para abertura da sessão pública.

14.5 - Decairá do direito de impugnar os termos deste Edital a licitante que não o fizer no prazo previsto no subitem anterior, não revestindo natureza de recurso as alegações apresentadas por empresa que, tendo aceitado sem objeção o instrumento convocatório, venha, após julgamento desfavorável, alegar falhas ou irregularidades que o viciariam.

14.6 - A impugnação, feita tempestivamente, será decidida pela Pregoeira, no prazo máximo de 02 (dois) dias úteis, contados da data do recebimento da impugnação.

15 - DA DOTAÇÃO ORÇAMENTÁRIA

15.1 - As despesas decorrentes da contratação do objeto da presente licitação correrão à conta de recursos específicos consignados no orçamento do Tribunal Regional Federal da Primeira Região ou a ele provisionados, os quais serão discriminados na respectiva Nota de Empenho.

16 - DAS DISPOSIÇÕES FINAIS

16.1 - Independentemente de declaração expressa, a simples apresentação de proposta implica na plena aceitação das condições estipuladas neste Edital e seus Anexos, bem como, do previsto na alínea "d" inciso II, art. 11 Lei nº 13.709, de 14.08/2018 (Lei Geral de Proteção de Dados - LGPD).

16.2 - O Tribunal Regional Federal da Primeira Região poderá adiar ou revogar a presente licitação, por interesse público decorrente de fato superveniente, devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado, ficando nesse último caso, desobrigado de indenizar, ressalvado o disposto no parágrafo único do art. 50 do Decreto 10.024/2019.

16.3 – Toda e qualquer comunicação/informação/notificação e envio de documentos (ata, contrato, nota de empenho e demais documentos) à licitante será feita pelo e-mail cadastrado no Portal de Compras do Governo Federal, ou outro que o substitua, apontado formalmente em sua proposta.

16.3.1 – É de exclusiva responsabilidade da licitante o fornecimento e manutenção de e-mail atualizado.

16.3.2 – Em caso de inobservância do previsto no subitem 16.3.1, o Tribunal Regional Federal da 1ª Região poderá realizar a comunicação/informação/notificação/intimação via postal/pessoal.

16.3.3 – Frustradas as tentativas na forma do subitem 16.3.2, o Tribunal Regional Federal da 1ª Região poderá realizar a comunicação/informação/notificação/intimação da licitante mediante publicação no Diário da Justiça Federal da 1ª Região – e-DJF1, disponível no site do Contratante (http://portal.trf1.jus.br/portaltrf1/publicacoes/diarios-da-justica/diarios-da-justica.htm), para todos os efeitos, ressalvadas as hipóteses legais em que se determine publicação no Diário Oficial da União.

16.4 - Alterações das condições deste Edital, bem como informações adicionais, serão divulgadas na *homepage* do Tribunal e no Portal de Compras do Governo Federal (www.trf1.jus.br e https://www.gov.br/compras/pt-br/), ficando as licitantes obrigadas a acessá-las para ciência.

16.5 - Os pedidos de esclarecimentos deverão ser enviados em até 03 (três) dias úteis anteriores à data fixada para a abertura do Certame, exclusivamente por meio eletrônico (dilit@trf1.jus.br).

16.5.1 – Os pedidos de esclarecimentos, feitos tempestivamente, serão respondidos pela Pregoeira, no prazo máximo de 02 (dois) dias úteis, contados da data do recebimento dos pedidos.

16.6 – ATENÇÃO: Fica instituída a assinatura eletrônica de documentos, conforme Resolução PRESI SECGE 16, de 03/09/2014. Para tanto, **os representantes das empresas vencedoras, indicados conforme alínea "b" do subitem 4.2 (DO ENVIO DAS PROPOSTAS),** após a homologação do Certame, **deverão obrigatoriamente**, se cadastrar, **no prazo de 05 (cinco) dias úteis**, no acesso externo do **Sistema Eletrônico de Informações (SEI)** no endereço:

https://sei.trf1.jus.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0, **para assinatura digital da Ata de Registro de Preços e/ou Contrato**, sob pena de aplicação das penalidades previstas nos subitens 13.3 e 13.4.1 deste Edital.

16.6.1 - Após o cadastro no SEI as respectivas unidades poderão disponibilizar o acesso para a licitante assinar os documentos, nos prazos estipulados neste Edital.

16.7 – Maiores informações poderão ser obtidas na Divisão de Licitações do Tribunal Regional Federal da Primeira Região, localizada no 2º Andar do Ed. Anexo I - SAS Quadra 01 Bloco C, Brasília/DF, CEP 70.070-900, telefones (61) 3410-3411 / 3410-3412 ou 3410-3414.

16.8 - Integram o presente Edital, independentemente de qualquer transcrição, os seguintes Anexos:

ANEXO I – SÍNTESE DO TERMO DE REFERÊNCIA;

ANEXO II – MODELO DE PLANILHA PARA FORMULAÇÃO DE PREÇOS;

ANEXO III – MODELO DE FORMULÁRIO DE AVALIAÇÃO TÉCNICA;

ANEXO IV – MINUTA DA ATA DE REGISTRO DE PREÇOS;

ANEXO V - MINUTA DE CONTRATO.

Brasília-DF, 29 de agosto de 2022.

ELIZETE FERREIRA COSTA:80452809 1

Assinado de forma digital por ELIZETE FERREIRA COSTA:80452809 1
Dados: 2022.08.29 15:26:34 -03'00'

Elizete Ferreira Costa
Pregoeira

ANEXO I - PREGÃO ELETRÔNICO SRP Nº 24/2022

SÍNTESE DO TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. O presente termo tem por objeto a contratação de empresa especializada no fornecimento, desinstalação, instalação e configuração de licenciamento de solução de antivírus, com garantia e atualização de versões, pelo período de 60 (sessenta) meses, bem como serviços de suporte especializado e treinamento, para as estações de trabalho e equipamentos servidores da Justiça Federal da 1ª Região, conforme quantidades e especificações constantes neste Anexo.

2. DA JUSTIFICATIVA

2.1. O Tribunal Regional Federal da 1ª Região, as Seções e Subseções Judiciárias que compõem a Justiça Federal da Primeira Região lidam diariamente com uma grande diversidade de informações. Em determinadas ocasiões, há que se preservar o seu sigilo e, de forma geral, deve-se assegurar a integridade e disponibilidade das informações.

2.2. Observa-se a necessidade de gerenciamento centralizado dando visibilidade ao administrador da solução sobre todos os problemas e ameaças que estão em curso ou foram eliminadas do ambiente. Soluções não corporativas, como as destinadas aos usuários residenciais não são suficientes para as necessidades da Justiça Federal da Primeira Região, visto que não possuem mecanismo centralizado de gerência e impossibilitam automação de execução das tarefas de instalação, configuração e atualização do antivírus

2.3. Grande parte das informações produzidas ou custodiadas na Justiça Federal da Primeira Região é armazenada em repositórios centralizados, tais como servidores de arquivos ou bancos de dados. Neste contexto, qualquer computador desprotegido pode representar riscos à segurança destas informações que serão acessadas e manipuladas por todos. Assim, torna-se imperioso o estabelecimento de mecanismos de proteção.

2.4. Tais mecanismos de proteção são particularmente relevantes quando a informação é acessada em sítios de internet, arquivos e dispositivos portáteis, que estão sujeitos a “infecção” em ambientes alheios ao Tribunal Regional Federal da Primeira Região (TRF1), Seções Judiciárias e Subseções Judiciárias da Justiça Federal da Primeira Região (JF1).

2.5. A segurança da informação é uma vertente cada vez mais necessária na composição da gestão de companhias e órgãos públicos, pois para além da crescente complexidade dos sistemas de negócio das empresas existe também

uma grande necessidade de proteção dos ativos organizacionais. Em paralelo, cumpre destacar que a indústria do cibercrime é um ramo de negócio cada vez mais promissor e que acarreta em significativos prejuízos para as mais diversas áreas empresariais e governamentais no Brasil e mundo.

2.6. Dentre as diversas áreas envolvidas para a realização de roubos, fraudes, danos e ataques aos diversos ramos de negócios no mundo todo destaca-se a indústria do malware, cuja complexidade dos produtos vem aumentando vertiginosamente, estando sempre passos à frente ao mercado de segurança cibernética. Dentre as tecnologias empregadas por hackers, em sua tentativas de invasão, estão inclusos mecanismos de inteligência artificial e de ocultação para burlarem a detecção de sistemas de segurança, como antimalwares e firewalls.

2.7. Nos últimos anos as entidades governamentais no mundo todo vêm sofrendo diversos ataques no âmbito digital, incluindo ataques de negação de serviço, roubo de informações, alterações de páginas e de dados, ataques direcionados e persistentes. Estes eventos contribuem para um enorme prejuízo em relação às suas imagens públicas, pois tais entidades prestam serviços à sociedade como um todo e mantêm na sua base inúmeros dados pessoais da população.

2.8. Para proteção do cidadão vem sendo necessário que os órgãos públicos façam investimentos cada vez mais em mecanismos mais robustos de proteção cibernética e dentre estes mecanismos se destacam as modernas soluções antimalwares. Computadores de usuários em uma instituição sempre foram considerados pontos de entrada para malwares e como cada vez mais as organizações têm liberado acesso à internet por parte de seu corpo funcional, a superfície de contato para execução de tais aplicativos maliciosos é cada vez maior.

2.9. Tudo isso implica em uma atenção especial ao monitoramento e proteção das estações de trabalho e dos equipamentos servidores da organização, sendo essencial a aquisição de uma ferramenta moderna a fim de evitar pontos de vulnerabilidades na rede, possibilitando a geração de relatórios ou consultas a fim de prover informações úteis ao gerenciamento do parque, possibilitando ações preventivas e reativas.

2.10. Outro ponto de fundamental importância é que essa ferramenta seja dotada de uma gerência centralizada, de forma que seja possível conduzir a administração de todo o parque antimalware garantindo que as políticas e atualizações ocorram de forma imediata a todos os nós da rede protegida, bem como logística de instalação simplificada.

2.11. Ademais, a prorrogação contratual, mesmo que fosse possível a extensão da garantia da solução atualmente em uso, não possibilitaria a obtenção de benefícios relacionados às inovações e modernizações da solução, para proteção

aos casos mais recentes de ataques realizados no âmbito da Administração Pública.

2.12. A Justiça Federal da Primeira Região (JF1) é composta pelo TRF1, Seções Judiciárias e Subseções Judiciárias, onde foi contabilizado um total máximo de 16.231 equipamentos ativos, no período de 10/2019 a 05/2020.

2.13. Deste modo, prover solução de antivírus nas quantidades supramencionadas é medida que se impõe para salvaguarda e segurança do ambiente tecnológico, pois sem a referida solução os riscos de ataques e suas consequências seriam ainda mais graves, podendo impactar, usuários internos e externos, inclusive os jurisdicionados.

3. DETALHAMENTO DO OBJETO/QUANTIDADES PARA REGISTRO DE PREÇOS

GRUPO	ITEM	SICAM	ESPECIFICAÇÃO	BR SIASG	UN	QUANTIDADE		
						POR ÓRGÃO		QUANT. TOTAL
01	01	52.35.005.017	**Solução de antivírus com licenciamento perpétuo, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses**	27472	LICENÇA	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	**12.784**	**19.284**
						SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	**3.500**	
						FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS	**3.000**	
	02	52.35.005.018	**Solução de antivírus com licenciamento perpétuo, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses**	27464	LICENÇA	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	**2.472**	**3.122**
						SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	**450**	
						FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS	**200**	
	03	52.35.005.018	**Suporte especializado - para**	26980	MESES	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	**12**	**36**

			licenciamento perpétuo, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses			SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	**12**	
						FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS	**12**	
	04	52.35.005.020	**Treinamento com licenciamento perpétuo, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses**	3840	ALUNOS	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	**10**	**26**
						SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	**06**	
						FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS	**10**	

GRUPO	**ITEM**	**SICAM**	**ESPECIFICAÇÃO**	**BR SIASG**	**UN**	**QUANTIDADE**		
						POR ÓRGÃO		**QUANT. TOTAL**
02	05	52.35.005.017	**Solução de antivírus com licenciamento por meio de subscrição, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses**	27502	LICENÇA	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	**12.784**	**19.284**
						SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	**3.500**	
						FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS	**3.000**	
	06	52.35.005.018	**Solução de antivírus com licenciamento por meio de subscrição, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60**	27502	LICENÇA	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	**2.472**	**3.122**
						SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	**450**	

			meses			FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS	**200**	
	07	52.35.005.018	**Suporte especializado - para licenciamento por meio de subscrição, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses**	26980	MESES	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	**12**	**36**
						SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	**12**	
						FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS	**12**	
	08	52.35.005.020	**Treinamento – para licenciamento por meio de subscrição, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses**	3840	ALUNOS	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	**10**	**26**
						SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	**06**	
						FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS	**10**	

3.1. Os Grupos 1 e 2 possuem a mesma solução com os mesmos quantitativos registrados pois tratam-se de tipo de licenciamento distintos que foram assim distribuídos para ampliação da concorrência, este Tribunal irá homologar somente o lote de menor preço, devendo após aceitação da melhor proposta, cancelar o grupo que restar com o maior valor.

3.2. Como as quantidades são meramente estimativas, não se constitui nenhum compromisso de consumo mínimo por parte do CONTRATANTE e nem poderão ser utilizadas como justificativa pela CONTRATADA para eventual alegação de prejuízo em razão de expectativa não satisfeita.

4. PRAZOS E ENTREGA DOS SERVIÇOS

4.1. As licenças deverão ser disponibilizadas, na última versão do software, por meio de chave de acesso no site da fabricante a ser enviada via e-mail para: TRF1 - sesei@trf1.jus.br; SJMG - nutec.mg@trf1.jus.br; e UFT - nati@uft.edu.br ou aislan@uft.edu.br, no prazo máximo de 10 (dez) dias úteis, contados do recebimento da Ordem de Fornecimento.

4.1.1. Deverão ser entregues juntamente com as chaves de acesso a documentação técnica e os manuais pertinentes aos softwares adquiridos.

4.1.2. A Validação das licenças entregues será por meio de visualização na console de gerenciamento da solução, que deverá estar disponível para o cliente.

4.2. Os serviços de desinstalação, instalação e configuração deverão ser executados, no prazo máximo de 44 (quarenta e quatro) dias úteis, contados do aceite provisório dos itens 1, 2, 5 e 6.

4.2.1. Entende-se por entrega da solução, objetos dos itens 1, 2, 5 e 6, a desinstalação e instalação e configuração das licenças.

4.2.2. Deverão ser iniciados os prazos de garantia e atualização das licenças, após o aceite definitivo.

4.3. O serviço de suporte deverá ser iniciado após assinatura do termo de recebimento definitivo dos Itens 1, 2, 5 e 6.

4.4. O serviço de treinamento deverá ser iniciado, no prazo máximo de 10 (dez) dias úteis, contados do recebimento da ordem de execução de serviço.

4.4.1. O serviço de treinamento deverá ser finalizado com o prazo máximo de até 10 (dez) dias úteis, contatos a partir do inicio do treinamento.

4.5. Para execução dos serviços de instalação e suporte técnico a CONTRATADA deverá entrar em contato com a equipe de fiscalização do contrato ou via e-mail para: TRF1 - sesei@trf1.jus.br; SJMG - nutec.mg@trf1.jus.br; e UFT - nati@uft.edu.br para que o CONTRATANTE disponibilize os meios de acesso remoto ao ambiente tecnológico.

4.6. O treinamento deverá ser prestados de forma remota, devendo a CONTRATADA enviar via e-mail para: TRF1 - sesei@trf1.jus.br; SJMG - nutec.mg@trf1.jus.br; e UFT - nati@uft.edu.br o link de acesso.

5. DA ESPECIFICAÇÃO TÉCNICA

5.1. SOLUÇÃO DE ANTIVÍRUS PARA ESTAÇÕES DE TRABALHO – LICENÇA PERPÉTUA

5.1.1. Características gerais:

5.1.1.1. Entende-se por agente ou antivírus como sendo a ferramenta de proteção contra malwares ou vírus, termo a ser usado tanto para os componentes de proteção de estações de trabalho ou equipamentos servidores;

5.1.1.2. A Solução deverá ser baseada na arquitetura cliente/servidor, sendo composta por componente de gerência centralizada única e agentes antivírus:

5.1.1.2.1. O serviço de gerência centralizada deverá ser ofertado, preferencialmente, a partir da nuvem. Caso o fornecedor oferte serviço de gerência centralizada de solução on-premise, essa deverá ser disponibilizada por meio de appliance virtual do mesmo fabricante da solução ofertada ou a Contratada deverá realizar a instalação e configuração do(s) servidor(es) no ambiente disponibilizado, sem custo adicional para o Contratante;

5.1.1.2.2. O tráfego de dados entre os agentes e gerência centralizada deverá ocorrer através de conexão segura;

5.1.1.2.3. Os componentes da solução deverão manter compatibilidade com o ambiente tecnológico da Justiça Federal da 1ª Região - JF1, conforme descrito no item 06 deste Anexo;

5.1.1.3. A solução deverá permitir instalação dos agentes de forma remota, abrangendo todas as Seções e Subseções;

5.1.1.4. A solução deverá ser fornecida pronta para utilização imediata da JF1, não sendo permitida apresentação de qualquer procedimento que configure o desenvolvimento da solução após a contratação;

5.1.1.5. A solução deverá ser de um único fabricante, não devendo ser composta por módulos, softwares, scripts ou plug-ins de terceiros;

5.1.1.5.1. Ressalvados os casos em que a solução ofertada utilize módulos do próprio Sistema Operacional, como Firewall e recursos de proteção antimalware nativos;

5.1.1.6. A solução deverá oferecer proteção em camadas para detecção de malwares;

5.1.1.7. O fabricante deverá oferecer serviço de análise e criação de solução específica para quando for identificado um possível malware não detectado pela solução antivírus;

5.1.1.8. Entende-se por licença perpétua aquela que após o encerramento do contrato de suporte firmado pela administração publica, permanecerá funcionando, até que o fabricante informe que as licenças não receberão suporte e atualização.

5.1.2. Gerenciamento centralizado:

5.1.2.1. A console de gerência centralizada deverá oferecer interface baseada em modo gráfico (GUI) acessível por software ou navegador web de forma segura (HTTPS);

5.1.2.2. Permitir o gerenciamento, controle, configuração e operação de todo parque (produtos instalados nos clientes e quaisquer outros módulos que componham a solução) de forma remota e centralizada;

5.1.2.3. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no item 06 deste Anexo;

5.1.2.4. Deverá permitir acessos simultâneos de vários usuários à console da gerência (sessões);

5.1.2.5. Deverá possuir uma base de dados centralizada para armazenamento das informações e logs dos clientes e da gerência;

5.1.2.6. Deverá permitir a criação e distribuição de políticas e tarefas remotamente para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

5.1.2.7. Deverá permitir operações de instalação, desinstalação e atualização dos módulos da solução para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

5.1.2.8. Oferecer mecanismo de comunicação (via push) entre o(s) servidor(es) e os clientes para entrega de dados e informações;

5.1.2.9. Oferecer mecanismo de comunicação (via pull) entre os clientes e o(s) servidor(es) para consulta de dados e informações de forma randômica;

5.1.2.10. A instalação ou atualização dos módulos componentes da solução, distribuição de configurações, políticas e tarefas da gerência aos clientes deve ser realizada de forma silenciosa e sem necessidade de reinicialização ou logoff do equipamento e sem necessidades de aguardar alguma ação do usuário do equipamento;

5.1.2.11. Deverá oferecer funcionalidade de execução, criação e customização de consultas às informações contidas na base de dados;

5.1.2.11.1. Deverá possibilitar a disponibilização das informações em modo de gráficos ou tabelas;

5.1.2.11.2. Deverá ser possível exportar as informações obtidas nas consultas em pelo menos um desses formatos: PDF, HTML, TXT, CSV ou Json;

5.1.2.11.3. Deverá permitir criação de alertas e notificação de eventos para administradores e usuários determinados;

5.1.2.11.4. Deverá possibilitar pesquisa no histórico de eventos;

5.1.2.11.5. Deverá permitir execução de consultas por agendamento e envio do resultado via email;

5.1.2.12. Deverá disponibilizar as seguintes consultas pré-definidas:

5.1.2.12.1. Máquinas com maior número de ocorrência de vírus e ameaças;

5.1.2.12.2. Usuários com maior número de ocorrência de vírus e ameaças;

5.1.2.12.3. Histórico de infecções nas últimas 24 horas, 7 dias e 30 dias;

5.1.2.12.4. Vírus e ameaças com maior número de registros nas últimas 24 horas, 7 dias e 30 dias;

5.1.2.12.5. Versões dos produtos instalados;

5.1.2.12.6. Versões das vacinas, quando for o caso, ou outras políticas de proteção adotadas.

5.1.2.13. Deverá permitir criação de dashboards;

5.1.2.14. Deverá permitir integração com o Active Directory da JF1 para descoberta de equipamentos ou de forma nativa na própria solução;

5.1.2.14.1. Deverá dar suporte a estrutura de florestas/domínios e subdomínios do Active Directory, refletindo a estrutura hierárquica da JF1 no Active Directory: TRF1 > Seções Judiciárias > Subseções Judiciárias.

5.1.2.15. Deverá permitir visualização ou agrupamento dos agentes instalados e gerenciados de forma a refletir a estrutura hierárquica da JF1, na forma representada no Active Directory, observando a ordem: Tribunal Regional Federal da 1ª Região - TRF1 > Seção Judiciária > Subseção Judiciária, seguindo a representação da Figura 1: Mapa Arquitetural, constante do subitem 6.4 deste Anexo;

5.1.2.16. Deverá ser capaz de distinguir e agrupar equipamentos servidores, estações de trabalho e notebooks, de forma a definir agrupamentos distintos para aplicação de regras, tarefas e políticas;

5.1.2.17. Deverá permitir que se configure diferentes políticas e tarefas para diferentes agrupamentos de computadores, seja para pontos

específicos na estrutura em árvore (Seção, Subseção) como para demais grupos específicos (servidores ou estações de trabalho);

5.1.2.18. Deverá possibilitar função de herança de políticas e tarefas entre os grupos e subgrupos, com possibilidade de quebra de herança;

5.1.2.19. O acesso à console da gerência centralizada deverá ser efetuado mediante autenticação segura através de usuário cadastrado na base de dados da solução ou através de autenticação integrada com usuários do Active Directory;

5.1.2.20. Todas as ações realizadas pelos usuários da gerência deverão ser registradas em log de auditoria, com no mínimo descrição da ação, nome do usuário, data e hora da ação realizada:

5.1.2.20.1. No caso de gerência em nuvem a solução deverá prover retenção de log por no mínimo 3 (três) meses online e possibilitar sua exportação.

5.1.2.20.2. No caso de gerência on-premise a solução deverá possibilitar criar backup da base de dados.

5.1.2.21. Deve permitir cadastro de usuários com, pelo menos, os seguintes perfis (ou equivalentes):

5.1.2.21.1. Administradores, com acesso a todas as funcionalidades da gerência e em toda a estrutura hierárquica da JF1;

5.1.2.21.2. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da JF1;

5.1.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da JF1 ou pontos específicos;

5.1.2.22. Deverá permitir instalação e desinstalação remota dos agentes antivírus, através da console de gerenciamento;

5.1.2.23. A solução deverá ser capaz de detectar e listar equipamentos conectados na rede e que não possuam a solução instalada;

5.1.2.24. Deverá identificar através da integração com o Active Directory, ou de forma nativa pela própria solução, computadores sem o agente antivírus instalado;

5.1.2.25. Deverá apresentar a funcionalidade de instalação da solução nos equipamentos detectados através da listagem de equipamentos sem o antivírus instalado ou por meio do Active Directory ou por orquestradores.

5.1.2.26. Deverá possibilitar o download de pacotes executáveis de instalação para proceder com instalação manual nos equipamentos, observado os sistemas operacionais suportados;

5.1.2.27. Deverá permitir limpeza automática de agentes inativos por determinado período de tempo, liberando as respectivas licenças;

5.1.2.28. No caso da solução em nuvem, a plataforma deverá ser certificada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes);

5.1.2.29. Deverá ser possível criação de políticas para distribuição de atualizações para o parque gerenciado com periodicidade mínima diária;

5.1.2.30. Deverá ser possível criação de políticas para distribuição de atualizações e vacinas para o parque gerenciado com periodicidade mínima diária;

5.1.2.31. Deverá permitir configuração alternativa para permitir que o agente busque atualização na nuvem do fabricante quando estiver fora do escopo da gerência centralizada;

5.1.2.32. As atualizações deverão ser do tipo incremental;

5.1.2.33. Deverá permitir distribuição de versões diferentes da solução para diferentes grupos de equipamentos;

5.1.2.33.1. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, restaurar e excluir;

5.1.2.34. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, limpar e excluir;

5.1.2.35. Deverá possibilitar restauração manual de arquivos quarentenados;

5.1.2.36. Deverá permitir criar listas de exclusões ou exceções para determinados aplicativos ou diretórios e subdiretórios;

5.1.2.37. Deverá utilizar os recursos locais de forma otimizada, sem impacto no desempenho do endpoint, ou possibilitar a configuração de baixo uso de recurso do dispositivo nas operações do agente antivírus;

5.1.2.38. Deverá permitir criação de políticas para bloqueio de dispositivos de armazenamento externos;

5.1.2.39. Deverá possibilitar extração de informações sobre dispositivos bloqueados, contendo no mínimo data e hora do ocorrido, equipamento onde o bloqueio ocorreu, rótulo do dispositivo bloqueado e usuário do sistema operacional logado durante o bloqueio;

5.1.2.40. Deverá fornecer solução Sandbox, em nuvem ou on-premise, para análise de malwares e mecanismo de reputação de softwares.

5.1.2.40.1. Em caso de fornecimento do Sandbox on-premise a Contratada deverá instalar e fornecer todos os recursos logísticos e de infraestrutura necessários para implantação do equipamento no ambiente do Contratante, a exemplo de alimentação elétrica, cabeamento, sem custo adicional.

5.1.2.40.2. As funcionalidades do serviço de Sandbox deverão ser integrados na gerência centralizada;

5.1.2.41. Deverá possibilitar aplicar bloqueios e respostas para ameaças detectadas e analisadas pelo serviço de Sandbox em todo o parque;

5.1.2.42. Deverá apresentar interface para investigação usando funcionalidades de Detecção e Resposta, sendo possível tomar ações para os equipamentos em análise;

5.1.3. Serviço de Desinstalação

5.1.3.1. A desinstalação do parque atual existente na JF1 deverá ser efetuada pela CONTRATADA;

5.1.3.2. A CONTRATANTE deverá fornecer as credenciais necessárias para a execução da desinstalação, como usuário com privilégio.

5.1.3.3. A estratégia a ser adotada na execução da desinstalação será previamente acordada entre o CONTRATANTE e a CONTRATADA.

5.1.3.4. A desinstalação da ferramenta existente deverá ocorrer de forma silenciosa para o usuário, sem necessitar de reboot do equipamento e sem solicitar ações do usuário da estação/servidor;

5.1.3.4.1. Em casos específicos onde seja necessário reboot, deverá ser informado para a CONTRANTE para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar;

5.1.3.5. O equipamento onde for instalado a nova solução deverá estar LIMPA e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações

em que mais de 1 solução além da vigente por este certame estejam instaladas no equipamento ao mesmo tempo;

5.1.3.6. Problemas na execução da desinstalação do agente deverão ser imediatamente comunicadas a CONTRATANTE;

5.1.4. Serviço de instalação e configuração

5.1.4.1. A instalação deverá ocorrer em todo o âmbito da JF1;

5.1.4.2. A instalação do agente deverá pressupor desinstalação da solução anterior;

5.1.4.3. A instalação do agente deverá ser imperceptível para o usuário, de forma a não aparecer pop-ups, mensagens, caixas de diálogos solicitando ação de usuário e nem janelas modais, de forma a interromper de qualquer forma o usuário;

5.1.4.4. Os serviços de instalação devem compreender a configuração da gerência centralizada em nuvem ou a configuração dos equipamentos servidores virtuais para os componentes da solução on-premise, incluindo appliance virtual da gerência centralizada, banco de dados da solução e demais componentes a serem utilizados pela solução de gerência;

5.1.4.5. Deverá possibilitar a instalação dos componentes da solução de forma a refletir a estrutura hierárquica da JF1, observando a ordem: TRF1 > Seção Judiciária > Subseção Judiciária e o gráfico arquitetural Figura 1: Mapa Arquitetural, constante do subitem 6.4 deste Anexo;

5.1.4.6. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as Seções e Subseções;

5.1.4.7. Deve permitir que se instale os agentes individualmente por computador ou em lote, para vários computadores;

5.1.4.8. A interoperabilidade entre os componentes da solução deverá ser configurada por políticas na gerência e utilizando protocolos seguros;

5.1.4.9. Deverá permitir que se programe através de políticas o agendamento da distribuição dos itens atualizados na gerência centralizada para os repositórios;

5.1.4.10. Ao final do processo de instalação a CONTRATADA deverá fornecer os seguintes relatórios:

5.1.4.10.1. Relação de todos os computadores contendo antivírus instalado, com no mínimo as seguintes informações, agrupados por localidade – Subseção/Seção/TRF1;

5.1.4.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção/Seção/TRF1, contendo no mínimo:

5.1.4.10.2.1. Versão de cada módulo da solução instalado;

5.1.4.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

5.1.4.10.2.3. Versão de demais bibliotecas ou catálogos que compõem a solução instalado;

5.1.4.10.2.4. Os relatórios serão utilizados para avaliar conformidade da prestação do serviço de instalação;

5.1.4.10.2.5. Serão comparados com o quantitativo de máquinas ativas na JF1, utilizando a seguinte fórmula para apurar o índice de instalação:

5.1.4.10.2.5.1. IND – Índice de instalação;

5.1.4.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

5.1.4.10.2.5.3. QLA – Quantidade licenças adquiridas;

5.1.4.10.2.5.4. Será dado aceite da solução quando o resultado da instalação IND possua valor igual ou superior a 0.8 – IND >= 0.8;

5.1.5. Solução de antivírus para estações de trabalho

5.1.5.1. Deverá ser compatível com as seguintes tecnologias de sistema operacional, no mínimo:

5.1.5.1.1. Windows 8.1;

5.1.5.1.2. Windows 10;

5.1.5.1.3. Linux CentOS;

5.1.5.1.4. Linux Debian;

5.1.5.2. Deverá proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares;

5.1.5.3. A solução e todos os seus componentes deverão funcionar como um agente composto por um executável único que será instalado na estação de trabalho, podendo encapsular os diversos módulos que compõe a solução;

5.1.5.3.1. Caso a solução utilize de recursos de segurança nativos do Sistema Operacional, os mesmos serão considerados como módulos do agente único utilizado;

5.1.5.3.2. O módulo EDR poderá ser disponibilizado através de um executável ou módulo separado ao da solução de antivírus;

5.1.5.4. Deverá ser capaz de reconhecer ataques e ações maliciosas por assinatura, por análise heurística ou por machine learning;

5.1.5.5. Soluções que usem somente método de detecção por assinatura não serão aceitas;

5.1.5.6. Deverá possuir mecanismo de análise comportamental;

5.1.5.7. Deverá ser capaz de proteger ataques provenientes de malwares;

5.1.5.8. Deverá ser capaz de realizar proteção contra ameaças mesmo estando o dispositivo não conectado à internet;

5.1.5.9. Quando o equipamento estiver fora da cobertura da gerência centralizada deverá ser capaz de buscar atualizações na internet, na nuvem do fabricante;

5.1.5.10. Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo e hash do arquivo;

5.1.5.11. Deverá ser capaz de detectar, alertar e prevenir quando for detectado alguma ameaça;

5.1.5.12. Deverá ser capaz de prover proteção contra-ataques que explorem vulnerabilidades do sistema operacional do host, de acordo com o estabelecido no item 5.1.5.1 deste Anexo;

5.1.5.13. Deverá possuir proteção contra BOTs e variantes;

5.1.5.14. Deverá efetuar proteção permanente e em tempo real dos processos em memória;

5.1.5.14.1. Processos suspeitos deverão ser bloqueados;

5.1.5.15. Deverá possuir mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados e contra ameaças avançadas e persistentes, que não são detectadas pelos métodos convencionais de antivírus;

5.1.5.16. Deverá ser capaz de detectar variações de malwares geradas em memória principal;

5.1.5.17. Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial do tipo Machine Learning;

5.1.5.18. Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação;

5.1.5.19. Deverá oferecer proteção contra-ataques de 0Day (dia zero);

5.1.5.20. Deverá oferecer proteção contra Ransomwares, com capacidade de avaliar processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos;

5.1.5.21. Deverá informar o nome ou endereço IP da origem do ataque ou infecção;

5.1.5.22. Deverá oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código Hash do executável, caminho e nome do aplicativo malicioso;

5.1.5.23. Deverá oferecer proteção contra vírus de macro e por scripts variados, incluindo bash e powershell;

5.1.5.24. Deverá oferecer mecanismo de bloqueio baseado em análise realizada pela central de inteligência do fabricante oriundo da nuvem;

5.1.5.25. Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas;

5.1.5.26. Deverá possibilitar visualizar toda a cadeia de ataque, inclusive os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros;

5.1.5.27. Deverá oferecer proteção para alterações suspeitas de registro;

5.1.5.28. Deverá prover mecanismos para criação proteções personalizadas para detecção;

5.1.5.29. Deverá oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção);

5.1.5.30. Deverá oferecer proteção contra-ataques direcionados;

5.1.5.31. Deverá gerar log local assim como enviá-los para a gerência;

5.1.5.32. Deverá permitir inclusão de exceções aplicações e caminhos;

5.1.5.33. A solução deverá oferecer proteção para ameaças em execução:

5.1.5.33.1. Na memória principal (RAM);

5.1.5.33.2. Em arquivos;

5.1.5.33.3. No tráfego de rede;

5.1.5.33.4. Em dados provenientes de browsers de navegação web (downloads, scripts, etc);

5.1.5.33.5. Em arquivos compactados (formatos zip, exe, cab, rar, etc);

5.1.5.33.6. Em processos de inicialização automática;

5.1.5.33.7. Em serviços criados/modificados;

5.1.5.34. Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados;

5.1.5.35. Deverá permitir bloqueio de alterações nas configurações do antivírus por parte do usuário, sendo permitido apenas por alterações de políticas ou mediante inserção de senha/password, definidos na gerência;

5.1.5.36. Deverá possibilitar a criação de lista de aplicações confiáveis (lista de exceções), a partir da gerência centralizada, para eliminação de detecções do tipo falso positivo;

5.1.5.36.1. Deverá oferecer a possibilidade de editar esta lista, com inclusão e remoção de aplicativos;

5.1.5.37. Deverá possuir a capacidade de detectar antivírus de outros fabricantes que possam acarretar incompatibilidade;

5.1.5.38. Deverá impedir execução e instalação de aplicativos cujo comportamento seja suspeito ou que constem na lista de aplicativos inseridos na gerência centralizada;

5.1.5.39. Deverá detectar e proteger em tempo real o computador contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de páginas da web e scripts em linguagens tais como javascript, vbscript, activex, etc;

5.1.5.40. Deverá oferecer mecanismo de controle de dispositivos externos;

5.1.5.41. A administração das regras da funcionalidade para controle mecanismos externos deverá ser realizada a partir da gerência centralizada;

5.1.5.42. O mecanismo de controle de dispositivos externos deverá possibilitar monitorar e bloquear dispositivos a partir de regras e políticas estabelecidas na gerencia centralizada, para no mínimo:

5.1.5.42.1. Dispositivos de rede externos (wifi portátil, dispositivos de dados móveis);

5.1.5.42.2. Transferências de dados para dispositivos mobile.;

5.1.5.42.3. Transferências de dados para dispositivos de armazenamento externos;

5.1.5.42.4. Possibilitar ações de bloqueio na execução de arquivos em transferência através de browsers e clientes de e-mail.

5.1.5.43. Deve oferecer ou executar uma das seguintes opções de ações corretivas para programas maliciosos detectados: bloquear o objeto, executar a limpeza da ameaça e executar ação de quarentena;

5.1.5.44. Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma que não seja perceptível aos seus usuários e nem influenciem negativamente no rendimento de aplicações em servidores;

5.1.5.45. No mínimo as seguintes ocorrências deverão ser registradas em arquivo de log local ou enviadas para a gerência centralizada:

5.1.5.45.1. Atualização de engine e/ou repositório de vacinas.

5.1.5.45.2. Recebimento de políticas e tarefas da gerência;

5.1.5.45.3. Inicialização e finalização de varreduras, agendadas ou manuais, ou quando realizada por meio de análise dos processos em tempo real baseado em machine learning;

5.1.5.45.4. Detecção de alguma ameaça, registrando no mínimo as seguintes informações:

5.1.5.45.4.1. Nome da ameaça;

5.1.5.45.4.2. Tipo da ameaça;

5.1.5.45.4.3. Arquivo ou local infectado;

5.1.5.45.4.4. Data e hora da detecção;

5.1.5.45.4.5. Mecanismo que gerou a detecção;

5.1.5.45.4.6. Nome da máquina/endereço IP;

5.1.5.45.4.7. Ação realizada;

5.1.5.45.4.8. Usuário logado no sistema;

5.1.5.46. Deverá buscar por itens de atualização nos repositórios, configurado pela gerência, de acordo com topologia e políticas especificadas;

5.1.5.47. Deverá possibilitar mais de uma versão da ferramenta e seus insumos, para que em casos de incompatibilidades decorrentes de atualizações, seja possível reinstalar versões anteriores estáveis ou instalar versões novas em grupos específicos, para fins de testes de compatibilidade antes de instalação em todo parque;

5.1.5.48. Deverá fornecer informações do status do agente e de seus componentes, através da gerência com informações atualizadas com delay máximo de 5 minutos;

5.1.5.49. Deve ser disponibilizado nos idiomas português, preferencialmente, ou inglês;

5.1.6. Garantia e atualização das licenças, para estações de trabalho

5.1.6.1. A garantia técnica deverá ser contratada junto ao fabricante da solução, e sua vigência não poderá ser inferior ao período de 60 (sessenta) meses, contados a partir da aceitação definitiva da solução;

5.1.6.2. O atendimento do serviço de suporte técnico da garantia, deverá ser feito por intermédio da CONTRATADA ou diretamente com a fabricante através de portal específico para fins de suporte ou por e-mail;

5.1.6.3. A garantia técnica deverá ser acionada nas situações específicas onde a CONTRATADA não conseguir solução para o problema ou quando o problema for detectado em relação aos elementos da solução contratada, tais como bugs ou algum mal funcionamento;

5.1.6.4. A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução;

5.1.6.5. As atualizações deverão ser fornecidas independente de solicitação da CONTRATANTE.

5.1.6.6. Deverão ser providas atualizações das listas de definições de vírus e demais insumos para funcionamento atualizado da solução, de acordo com o mercado;

5.1.6.7. Deverá permitir atualizações da engine do agente (software), assim como da base de dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução;

5.1.6.8. A garantia técnica contempla suporte técnico do fabricante, serviços de manutenções e atualizações da solução antivírus, base de dados de vacinas, bem como disponibilização de:

5.1.6.8.1. Solução de problemas que afetem elementos da solução, incluindo os softwares, atualizações e instalação, evoluções, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;

5.1.6.8.2. Manuais dos produtos e serviços ofertados, base de conhecimento para soluções conhecidas, canal de comunicação, esclarecimento de dúvidas e quaisquer outras informações solicitadas pela CONTRATANTE:

5.1.6.8.2.1. As informações prestadas deverão ser disponibilizadas preferencialmente no idioma Português do Brasil ou na falta deste, obrigatoriamente no idioma em Inglês;

5.1.6.8.3. Novas versões da solução lançadas pelo fabricante e lançamento de novos softwares em substituição da solução contratada, em caso de descontinuação do software fornecido.

5.1.6.9. Os serviços descritos neste item deverão ser prestados mediante abertura de chamado pela CONTRATANTE ou pela CONTRATADA, diretamente no portal de comunicação e suporte do fabricante, realizado por meio de e-mail e site de helpdesk;

5.1.6.10. A garantia deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia.

5.2. SOLUÇÃO DE ANTIVIRUS PARA SERVIDORES – LICENÇA PERPÉTUA

5.2.1. Características gerais:

5.2.1.1. Entende-se por agente ou antivírus como sendo a ferramenta de proteção contra malwares ou vírus, termo a ser usado tanto para os componentes de proteção de estações de trabalho ou equipamentos servidores;

5.2.1.2. A Solução deverá ser baseada na arquitetura cliente/servidor, sendo composta por componente de gerência centralizada e agentes antivírus:

5.2.1.2.1. O serviço de gerência centralizada deverá ser ofertado, preferencialmente, a partir da nuvem. Caso o fornecedor oferte serviço de gerência centralizada de solução on-premise, essa deverá ser disponibilizada por meio de appliance virtual do mesmo fabricante da solução ofertada ou a Contratada deverá realizar a instalação e configuração do(s) servidor(es) no ambiente disponibilizado, sem custo adicional para o Contratante;

5.2.1.2.2. O tráfego de dados entre os agentes e gerência centralizada deverá ocorrer através de conexão segura;

5.2.1.2.3. Os componentes da solução deverão manter compatibilidade com o ambiente tecnológico da Justiça Federal da 1ª Região - JF1, conforme descrito no item 06 deste Anexo;

5.2.1.3. A solução deverá permitir instalação dos agentes de forma remota, abrangendo todas as Seções e Subseções;

5.2.1.4. A solução deverá ser fornecida pronta para utilização imediata da JF1, não sendo permitida apresentação de qualquer procedimento que configure o desenvolvimento da solução após a contratação;

5.2.1.5. A solução deverá ser de um único fabricante, não devendo ser composta por módulos, softwares, scripts ou plug-ins de terceiros;

5.2.1.5.1. Ressalvados os casos em que a solução ofertada utilize módulos do próprio Sistema Operacional, como Firewall e recursos de proteção antimalware nativos;

5.2.1.6. A solução deverá oferecer proteção em camadas para detecção de malwares;

5.2.1.7. O fabricante deverá oferecer serviço de análise e criação de solução específica para quando for identificado um possível malware não detectado pela solução antivírus;

5.2.1.8. Entende-se por licença perpétua aquela que após o encerramento do contrato de suporte firmado pela administração publica, permanecerá funcionando, até que o fabricante informe que as licenças não receberão suporte e atualização.

5.2.2. Gerenciamento centralizado:

5.2.2.1. A console de gerência centralizada deverá oferecer interface baseada em modo gráfico (GUI) acessível por software ou navegador web de forma segura (HTTPS);

5.2.2.2. Permitir o gerenciamento, controle, configuração e operação de todo parque (produtos instalados nos clientes e quaisquer outros módulos que componham a solução) de forma remota e centralizada;

5.2.2.3. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no item 06 deste Anexo;

5.2.2.4. Deverá permitir acessos simultâneos de vários usuários à console da gerência (sessões);

5.2.2.5. Deverá possuir uma base de dados centralizada para armazenamento das informações e logs dos clientes e da gerência;

5.2.2.6. Deverá permitir a criação e distribuição de políticas e tarefas remotamente para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

5.2.2.7. Deverá permitir operações de instalação, desinstalação e atualização dos módulos da solução para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

5.2.2.8. Oferecer mecanismo de comunicação (via push) entre o(s) servidor(es) e os clientes para entrega de dados e informações;

5.2.2.9. Oferecer mecanismo de comunicação (via pull) entre os clientes e o(s) servidor(es) para consulta de dados e informações de forma randômica;

5.2.2.10. A instalação ou atualização dos módulos componentes da solução, distribuição de configurações, políticas e tarefas da gerência aos clientes deve ser realizada de forma silenciosa e sem necessidade de reinicialização ou logoff do equipamento e sem necessidades de aguardar alguma ação do usuário do equipamento;

5.2.2.11. Deverá oferecer funcionalidade de execução, criação e customização de consultas às informações contidas na base de dados;

5.2.2.11.1. Deverá possibilitar a disponibilização das informações em modo de gráficos ou tabelas;

5.2.2.11.2. Deverá ser possível exportar as informações obtidas nas consultas em pelo menos um desses formatos: PDF, HTML, TXT, CSV ou Json;

5.2.2.11.3. Deverá permitir criação de alertas e notificação de eventos para administradores e usuários determinados;

5.2.2.11.4. Deverá possibilitar pesquisa no histórico de eventos;

5.2.2.11.5. Deverá permitir execução de consultas por agendamento e envio do resultado via email;

5.2.2.12. Deverá disponibilizar as seguintes consultas pré-definidas:

5.2.2.12.1. Máquinas com maior número de ocorrência de vírus e ameaças;

5.2.2.12.2. Usuários com maior número de ocorrência de vírus e ameaças;

5.2.2.12.3. Histórico de infecções nas últimas 24 horas, 7 dias e 30 dias;

5.2.2.12.4. Vírus e ameaças com maior número de registros nas últimas 24 horas, 7 dias e 30 dias;

5.2.2.12.5. Versões dos produtos instalados;

5.2.2.12.6. Versões das vacinas, quando for o caso, ou outras políticas de proteção adotadas.

5.2.2.13. Deverá permitir criação de dashboards;

5.2.2.14. Deverá permitir integração com o Active Directory da JF1 para descoberta de equipamentos ou de forma nativa na própria solução;

5.2.2.14.1. Deverá dar suporte a estrutura de florestas/domínios e subdomínios do Active Directory, refletindo a estrutura hierárquica da JF1 no Active Directory: TRF1 > Seções Judiciárias > Subseções Judiciárias

5.2.2.15. Deverá permitir visualização ou agrupamento dos agentes instalados e gerenciados de forma a refletir a estrutura hierárquica da JF1, na forma representada no Active Directory, observando a ordem: Tribunal Regional Federal da 1ª Região - TRF1 > Seção Judiciária > Subseção Judiciária, seguindo a representação da Figura 1: Mapa Arquitetural, constante do subitem 6.4 deste Anexo;

5.2.2.16. Deverá ser capaz de distinguir e agrupar equipamentos servidores, estações de trabalho e notebooks, de forma a definir agrupamentos distintos para aplicação de regras, tarefas e políticas;

5.2.2.17. Deverá permitir que se configure diferentes políticas e tarefas para diferentes agrupamentos de computadores, seja para pontos

específicos na estrutura em árvore (Seção, Subseção) como para demais grupos específicos (servidores ou estações de trabalho);

5.2.2.18. Deverá possibilitar função de herança de políticas e tarefas entre os grupos e subgrupos, com possibilidade de quebra de herança;

5.2.2.19. O acesso à console da gerência centralizada deverá ser efetuado mediante autenticação segura através de usuário cadastrado na base de dados da solução ou através de autenticação integrada com usuários do Active Directory;

5.2.2.20. Todas as ações realizadas pelos usuários da gerência deverão ser registradas em log de auditoria, com no mínimo descrição da ação, nome do usuário, data e hora da ação realizada:

5.2.2.20.1. No caso de gerência em nuvem a solução deverá prover retenção de log por no mínimo 3 (três) meses online e possibilitar sua exportação.

5.2.2.20.2. No caso de gerência on-premise a solução deverá possibilitar criar backup da base de dados.

5.2.2.21. Deve permitir cadastro de usuários com, pelo menos, os seguintes perfis (ou equivalentes):

5.2.2.21.1. Administradores, com acesso a todas as funcionalidades da gerência e em toda a estrutura hierárquica da JF1;

5.2.2.21.2. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da JF1;

5.2.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da JF1 ou pontos específicos;

5.2.2.22. Deverá permitir instalação e desinstalação remota dos agentes antivírus, através da console de gerenciamento;

5.2.2.23. A solução deverá ser capaz de detectar e listar equipamentos conectados na rede e que não possuam a solução instalada;

5.2.2.24. Deverá identificar através da integração com o Active Directory, ou de forma nativa pela própria solução, computadores sem o agente antivírus instalado;

5.2.2.25. Deverá apresentar a funcionalidade de instalação da solução nos equipamentos detectados através da listagem de equipamentos sem o antivírus instalado ou por meio do Active Directory ou por orquestradores.

5.2.2.26. Deverá possibilitar o download de pacotes executáveis de instalação para proceder com instalação manual nos equipamentos, observado os sistemas operacionais suportados;

5.2.2.27. Deverá permitir limpeza automática de agentes inativos por determinado período de tempo, liberando as respectivas licenças;

5.2.2.28. No caso da solução em nuvem, a plataforma deverá ser certificada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes);

5.2.2.29. Deverá ser possível criação de políticas para distribuição de atualizações para o parque gerenciado com periodicidade mínima diária;

5.2.2.30. Deverá ser possível criação de políticas para distribuição de atualizações e vacinas para o parque gerenciado com periodicidade mínima diária;

5.2.2.31. Deverá permitir configuração alternativa para permitir que o agente busque atualização na nuvem do fabricante quando estiver fora do escopo da gerência centralizada;

5.2.2.32. As atualizações deverão ser do tipo incremental;

5.2.2.33. Deverá permitir distribuição de versões diferentes da solução para diferentes grupos de equipamentos;

5.2.2.33.1. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, restaurar e excluir;

5.2.2.34. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, limpar e excluir;

5.2.2.35. Deverá possibilitar restauração manual de arquivos quarentenados;

5.2.2.36. Deverá permitir criar listas de exclusões ou exceções para determinados aplicativos ou diretórios e subdiretórios;

5.2.2.37. Deverá utilizar os recursos locais de forma otimizada, sem impacto no desempenho do endpoint, ou possibilitar a configuração de baixo uso de recurso do dispositivo nas operações do agente antivírus;

5.2.2.38. Deverá permitir criação de políticas para bloqueio de dispositivos de armazenamento externos;

5.2.2.39. Deverá possibilitar extração de informações sobre dispositivos bloqueados, contendo no mínimo data e hora do ocorrido, equipamento onde o bloqueio ocorreu, rótulo do dispositivo bloqueado e usuário do sistema operacional logado durante o bloqueio;

5.2.2.40. Deverá fornecer solução Sandbox, em nuvem ou on-premise, para análise de malwares e mecanismo de reputação de softwares.

5.2.2.40.1. Em caso de fornecimento do Sandbox on-premise a Contratada deverá instalar e fornecer todos os recursos logísticos e de infraestrutura necessários para implantação do equipamento no ambiente do Contratante, a exemplo de alimentação elétrica, cabeamento, sem custo adicional.

5.2.2.40.2. As funcionalidades do serviço de Sandbox deverão ser integrados na gerência centralizada;

5.2.2.41. Deverá possibilitar aplicar bloqueios e respostas para ameaças detectadas e analisadas pelo serviço de Sandbox em todo o parque;

5.2.2.42. Deverá apresentar interface para investigação usando funcionalidades de Detecção e Resposta, sendo possível tomar ações para os equipamentos em análise;

5.2.3. Serviço de Desinstalação

5.2.3.1. A desinstalação do parque atual existente na JF1 deverá ser efetuada pela CONTRATADA;

5.2.3.2. A CONTRATANTE deverá fornecer as credenciais necessárias para a execução da desinstalação, como usuário com privilégio.

5.2.3.3. A estratégia a ser adotada na execução da desinstalação será previamente acordada entre o CONTRATANTE e a CONTRATADA.

5.2.3.4. A desinstalação da ferramenta existente deverá ocorrer de forma silenciosa para o usuário, sem necessitar de reboot do equipamento e sem solicitar ações do usuário da estação/servidor;

5.2.3.4.1. Em casos específicos onde seja necessário reboot, deverá ser informado para a CONTRANTE para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar;

5.2.3.5. O equipamento onde for instalado a nova solução deverá estar LIMPA e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações

em que mais de 1 solução além da vigente por este certame estejam instaladas no equipamento ao mesmo tempo;

5.2.3.6. Problemas na execução da desinstalação do agente deverão ser imediatamente comunicadas a CONTRATANTE;

5.2.4. Serviço de instalação e configuração

5.2.4.1. A instalação deverá ocorrer em todo o âmbito da JF1;

5.2.4.2. A instalação do agente deverá pressupor desinstalação da solução anterior;

5.2.4.3. A instalação do agente deverá ser imperceptível para o usuário, de forma a não aparecer pop-ups, mensagens, caixas de diálogos solicitando ação de usuário e nem janelas modais, de forma a interromper de qualquer forma o usuário;

5.2.4.4. Os serviços de instalação devem compreender a configuração da gerência centralizada em nuvem ou a configuração dos equipamentos servidores virtuais para os componentes da solução on-premise, incluindo appliance virtual da gerência centralizada, banco de dados da solução e demais componentes a serem utilizados pela solução de gerência;

5.2.4.5. Deverá possibilitar a instalação dos componentes da solução de forma a refletir a estrutura hierárquica da JF1, observando a ordem: TRF1 > Seção Judiciária > Subseção Judiciária e o gráfico arquitetural Figura 1: Mapa Arquitetural, constante do subitem 6.4 deste Anexo;

5.2.4.6. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as Seções e Subseções;

5.2.4.7. Deve permitir que se instale os agentes individualmente por computador ou em lote, para vários computadores;

5.2.4.8. A interoperabilidade entre os componentes da solução deverá ser configurada por políticas na gerência e utilizando protocolos seguros;

5.2.4.9. Deverá permitir que se programe através de políticas o agendamento da distribuição dos itens atualizados na gerência centralizada para os repositórios;

5.2.4.10. Ao final do processo de instalação a CONTRATADA deverá fornecer os seguintes relatórios:

5.2.4.10.1. Relação de todos os computadores contendo antivírus instalado, com no mínimo as seguintes informações, agrupados por localidade – Subseção/Seção/TRF1;

5.2.4.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção/Seção/TRF1, contendo no mínimo:

5.2.4.10.2.1. Versão de cada módulo da solução instalado;

5.2.4.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

5.2.4.10.2.3. Versão de demais bibliotecas ou catálogos que compõem a solução instalado;

5.2.4.10.2.4. Os relatórios serão utilizados para avaliar conformidade da prestação do serviço de instalação;

5.2.4.10.2.5. Serão comparados com o quantitativo de máquinas ativas na JF1, utilizando a seguinte fórmula para apurar o índice de instalação:

5.2.4.10.2.5.1. IND – Índice de instalação;

5.2.4.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

5.2.4.10.2.5.3. QLA – Quantidade licenças adquiridas;

5.2.4.10.2.5.4. Será dado aceite da solução quando o resultado da instalação IND possua valor igual ou superior a 0.8 – IND >= 0.8;

5.2.5. Solução de antivírus para equipamentos servidores

5.2.5.1. Deverá ser compatível com as seguintes tecnologias de sistema operacional, no mínimo:

5.2.5.1.1. Windows Server 2012;

5.2.5.1.2. Windows Server 2016;

5.2.5.1.3. Windows Server 2019 e posteriores;

5.2.5.1.4. Linux CentOS;

5.2.5.1.5. Linux Debian;

5.2.5.1.6. Linux Red Hat;

5.2.5.2. Deverá proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares;

5.2.5.3. A solução e todos os seus componentes deverão funcionar como um agente composto por um executável único que será instalado na

estação de trabalho, podendo encapsular os diversos módulos que compõe a solução;

5.2.5.3.1. Caso a solução utilize de recursos de segurança nativos do Sistema Operacional, os mesmos serão considerados como módulos do agente único utilizado;

5.2.5.4. Deverá ser capaz de reconhecer ataques e ações maliciosas por assinatura, por análise heurística ou por machine learning.

5.2.5.5. Soluções que usem somente método de detecção por assinatura não serão aceitas;

5.2.5.6. Deverá possuir mecanismo de análise comportamental;

5.2.5.7. Deverá ser capaz de proteger ataques provenientes de malwares;

5.2.5.8. Deverá ser capaz de realizar proteção contra ameaças mesmo estando o dispositivo não conectado à internet;

5.2.5.9. Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo e hash do arquivo;

5.2.5.10. Deverá ser capaz de detectar, alertar e prevenir quando for detectado alguma ameaça;

5.2.5.11. Deverá ser capaz de prover proteção contra ataques que explorem vulnerabilidades do sistema operacional do host, de acordo com o estabelecido no item 5.2.5.1 deste Anexo;

5.2.5.12. Deverá possuir proteção contra BOTs e variantes;

5.2.5.13. Deverá efetuar proteção permanente e em tempo real dos processos em memória;

5.2.5.13.1. Processos suspeitos deverão ser bloqueados;

5.2.5.14. Deverá possuir mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados e contra ameaças avançadas e persistentes, que não são detectadas pelos métodos convencionais de antivírus;

5.2.5.15. Deverá ser capaz de detectar variações de malwares geradas em memória principal;

5.2.5.16. Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial do tipo Machine Learning;

5.2.5.17. Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação;

5.2.5.18. Deverá oferecer proteção contra ataques de 0Day (dia zero);

5.2.5.19. Deverá oferecer proteção contra Ransomwares, com capacidade de avaliar processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos;

5.2.5.20. Deverá informar o nome ou endereço IP da origem do ataque ou infecção;

5.2.5.21. Deverá ter a capacidade de bloquear ataques direcionados a aplicações em execução no servidor através de funcionalidade de proteção contra vulnerabilidades conhecidas e catalogadas através de CVE ou catálogo próprio, tanto para o sistema operacional quanto para aplicações instaladas no servidor;

5.2.5.21.1. O mecanismo deverá proteger no mínimo os seguintes softwares de terceiros: Apache, Tomcat, JBoss, Microsft IIS, SQL Server, PostgreSQL, Banco de Dados Oracle, MySQL e variantes, Wordpress, Joomla, Adobe entre outros;

5.2.5.22. Em caso de ataque a solução deverá detectar comportamentos maliciosos da aplicação web;

5.2.5.23. Para sistemas operacionais windows a solução deverá gerenciar o seu Firewall ou possuir Firewall bidirecional com detecção e proteção contra intrusões e ataques.

5.2.5.23.1. Firewall deverá possibilitar ações como permitir e bloquear: portas, range de portas, IPs, range de IPs e redes;

5.2.5.23.2. Deverá ser possível aplicar regras de permitir todo tráfego ou bloquear todo tráfego;

5.2.5.24. Deverá oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código Hash do executável, caminho e nome do aplicativo malicioso;

5.2.5.25. Deverá oferecer proteção contra vírus de macro e por scripts variados, incluindo bash e powershell;

5.2.5.26. Deverá oferecer mecanismo de bloqueio baseado em análise realizada pela central de inteligência do fabricante oriundo na nuvem;

5.2.5.27. Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas

5.2.5.28. Deverá possibilitar visualizar toda a cadeia de ataque, inclusive os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros;

5.2.5.29. Deverá oferecer proteção para alterações suspeitas de registro;

5.2.5.30. Deverá prover mecanismos para criação proteções personalizadas para detecção;

5.2.5.31. Deverá oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção);

5.2.5.32. Deverá oferecer proteção contra ataques direcionados;

5.2.5.33. Deverá gerar log local assim como envia-los para a gerência, ou enviar logs em tempo real para a gerência centralizada;

5.2.5.34. Deverá permitir inclusão de exceções aplicações e caminhos;

5.2.5.35. A solução deverá oferecer proteção para ameaças em execução:

5.2.5.35.1. Na memória principal (RAM);

5.2.5.35.2. Em arquivos;

5.2.5.35.3. No tráfego de rede;

5.2.5.35.4. Em dados provenientes de browsers de navegação web (downloads, scripts, etc);

5.2.5.35.5. Em arquivos compactados (formatos zip, exe, cab, rar, etc);

5.2.5.35.6. Em processos de inicialização automática;

5.2.5.35.7. Em serviços criados/modificados;

5.2.5.36. Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados;

5.2.5.37. Deverá possibilitar a criação de lista de aplicações confiáveis (lista de exceções), a partir da gerencia centralizada, para eliminação de detecções do tipo falso positivo;

5.2.5.37.1. Deverá oferecer a possibilidade de editar esta lista, com inclusão e remoção de aplicativos;

5.2.5.38. Deverá possuir a capacidade de detectar antivírus de outros fabricantes que possam acarretar em incompatibilidade;

5.2.5.39. Deverá impedir execução e instalação de aplicativos cujo comportamento seja suspeito ou que constem na lista de aplicativos inseridos na gerência centralizada;

5.2.5.40. Deverá detectar e proteger em tempo real o computador contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de páginas da web e scripts em linguagens tais como javascript, vbscript, activex, etc;

5.2.5.41. Deve oferecer ou executar uma das seguintes opções de ações corretivas para programas maliciosos detectados: bloquear o objeto, executar a limpeza da ameaça e executar ação de quarentena;

5.2.5.42. Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma a não influenciar negativamente no rendimento de aplicações em servidores;

5.2.5.43. No mínimo as seguintes ocorrências deverão ser registradas em arquivo de log local ou enviadas para a gerência centralizada:

5.2.5.43.1. Atualização de engine e/ou repositório de vacinas.

5.2.5.43.2. Recebimento de políticas e tarefas da gerência;

5.2.5.43.3. Inicialização e finalização de varreduras, agendadas ou manuais, ou quando realizada por meio de análise dos processos em tempo real baseado em machine learning;

5.2.5.43.4. Detecção de alguma ameaça, registrando no mínimo as seguintes informações:

5.2.5.43.4.1. Nome da ameaça;

5.2.5.43.4.2. Tipo da ameaça;

5.2.5.43.4.3. Arquivo ou local infectado;

5.2.5.43.4.4. Data e hora da detecção;

5.2.5.43.4.5. Mecanismo que gerou a detecção (varredura agendada, manual, em tempo real);

5.2.5.43.4.6. Nome da máquina/endereço IP;

5.2.5.43.4.7. Ação realizada;

5.2.5.43.4.8. Usuário logado no sistema;

5.2.5.44. Deverá buscar por itens de atualização nos repositórios, configurado pela gerência, de acordo com topologia e políticas especificadas;

5.2.5.45. Deverá possibilitar mais de uma versão da ferramenta e seus insumos, para que em casos de incompatibilidades decorrentes de atualizações, seja possível reinstalar versões anteriores estáveis ou instalar versões novas em grupos específicos, para fins de testes de compatibilidade antes de instalação em todo parque;

5.2.5.46. Deverá fornecer informações do status do agente e de seus componentes, através da gerência com informações atualizadas com delay máximo de 5 minutos;

5.2.5.47. Deve ser disponibilizado nos idiomas: português (preferencialmente) ou inglês;

5.2.6. Garantia e atualização das licenças, para servidores

5.2.6.1. A garantia técnica deverá ser contratada junto ao fabricante da solução, e sua vigência não poderá ser inferior ao período de 60 (sessenta) meses, contados a partir da aceitação definitiva da solução;

5.2.6.2. O atendimento do serviço de suporte técnico da garantia deverá ser feito por intermédio da CONTRATADA ou diretamente com a fabricante através de portal específico para fins de suporte ou por e-mail;

5.2.6.3. A garantia técnica deverá ser acionada nas situações específicas onde a CONTRATADA não conseguir solução para o problema ou quando o problema for detectado em relação aos elementos da solução contratada, tais como bugs ou algum mal funcionamento;

5.2.6.4. A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução;

5.2.6.5. As atualizações deverão ser fornecidas independente de solicitação da CONTRATANTE.

5.2.6.6. Deverão ser providas atualizações das listas de definições de vírus e demais insumos para funcionamento atualizado da solução, de acordo com o mercado;

5.2.6.7. Deverá permitir atualizações da engine do agente (software), assim como da base de dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução;

5.2.6.8. A garantia técnica contempla suporte técnico do fabricante, serviços de manutenções e atualizações da solução antivírus, base de dados de vacinas, bem como disponibilização de:

5.2.6.8.1. Solução de problemas que afetem elementos da solução, incluindo os softwares, atualizações e instalação, evoluções, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;

5.2.6.8.2. Manuais dos produtos e serviços ofertados, base de conhecimento para soluções conhecidas, canal de comunicação, esclarecimento de dúvidas e quaisquer outras informações solicitadas pela CONTRATANTE:

5.2.6.8.2.1. As informações prestadas deverão ser disponibilizadas preferencialmente no idioma Português do Brasil ou na falta deste, obrigatoriamente no idioma em Inglês;

5.2.6.8.3. Novas versões da solução lançadas pelo fabricante e lançamento de novos softwares em substituição da solução contratada, em caso de descontinuação do software fornecido.

5.2.6.9. Os serviços descritos neste item deverão ser prestados mediante abertura de chamado pela CONTRATANTE ou pela CONTRATADA, diretamente no portal de comunicação e suporte do fabricante, realizado por meio de e-mail e site de helpdesk;

5.2.6.10. A garantia deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia.

5.3. SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO

5.3.1. O serviço de suporte técnico especializado deverá ser prestado pela CONTRATADA durante o prazo de 12 (doze) meses, contados a partir da aceitação definitiva da solução.

5.3.2. O atendimento do serviço de suporte técnico, incluindo telefone, e-mail, presencial ou outros que se fizerem necessários, deverá ser realizado no idioma Português do Brasil;

5.3.3. O serviço de suporte deverá incluir a operacionalização das atualizações do fabricante para a solução, assim como serviços de manutenções da solução antivírus, base de dados de vacinas, com garantia completa dos serviços prestados:

5.3.3.1. O serviço técnico deverá contemplar a solução de problemas que afetem elementos da solução, atualizações, problemas de instalação, evoluções, patches, aplicação e implantação de correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;

5.3.4. Os serviços descritos neste item deverão ser prestados mediante abertura de chamado pela CONTRATANTE, realizado por meio de contato telefônico 0800, e-mail e site de helpdesk, quando houver, e em regime 24x7:

5.3.4.1. Para cada serviço técnico prestado a CONTRATADA deverá fornecer um identificador para a chamada realizada, acompanhando o nome do responsável pelo tratamento do chamado;

5.3.4.2. Toda e qualquer ação realizada pela CONTRATADA no ambiente da CONTRATANTE só poderá ser realizada com anuência e autorização da CONTRATANTE e por meio de acompanhamento de representante indicado para tal fim;

5.3.5. A CONTRATADA deverá fornecer relatório mensal dos chamados efetuados ou de chamado específico, contendo a data e hora da abertura por chamado, data e hora de cada atendimento realizado, a descrição do problema abordado e das ações realizadas e data do fechamento do chamado, após aceite por parte da CONTRATANTE.

5.3.6. Os serviços de suporte técnico e manutenção deverão ser realizados na modalidade remota, conforme critérios estabelecidos:

5.3.7. Os chamados deverão ser classificados conforme a severidade, de acordo com as definições da tabela abaixo:

Categoria	Nível	Descrição
Urgente	1	Serviços totalmente indisponíveis. Falha em servidor de produção que deixe indisponível os recursos do mesmo (serviço parado). Impacto a múltiplos usuários e/ou falha em servidor de produção que afete operações críticas da JF-1.
Crítico	2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos. Falha intermitente em serviços suportados que torne o ambiente inoperante. Impacto individual ou a pequenos grupos. Operação normal afetada, mas sem interrupção.
Não Crítico	3	Serviços disponíveis com ocorrência de alarmes de avisos, consulta sobre problemas, dúvidas gerais sobre a ferramenta antivírus. Manutenção e monitoramento de eventos de falhas ou de avisos relatados pelo cliente. Pequeno impacto a um ou mais usuários. A correção pode ser feita de maneira agendada, em um momento futuro.

5.3.8. A CONTRATADA deverá atender os chamados com prazo de início e término de acordo com a tabela a seguir:

Modalidade	Prazos de Atendimento	Níveis de severidade		
		1-Urgente	2-Crítico	3-Não crítico
E-mail, remoto, ou telefone.	Início	2 horas	4 horas	8 horas
	Término	12 horas	24 horas	72 horas

5.3.9. Entende-se como término de atendimento a solução definitiva do incidente ou redução de sua criticidade, a partir do qual será considerado o prazo limite do novo nível de criticidade.

5.4. TREINAMENTO

5.4.1. Deverão ser abordados no treinamento, no mínimo, os seguintes assuntos:

5.4.1.1. Informações e conhecimento sobre arquitetura, funcionamento e componentes envolvidos na solução.

5.4.1.2. Conhecimento da usabilidade e operação da solução, envolvendo:

5.4.1.3. Instalação e configuração dos componentes da gerência.

5.4.1.4. Gerência de políticas, tarefas e demais atividades oferecidas pela gerência da solução (criação e configuração).

5.4.1.5. Instalação e configuração dos agentes.

5.4.1.6. Criação e execução de consultas e relatórios

5.4.2. O treinamento deve ser realizado de segunda a sexta-feira (dias úteis), entre 8h (oito) horas e 18h (dezoito) horas.

5.4.3. O treinamento deve ter carga horária mínima de 16 (dezesseis) horas, limitado a 4h/aula diárias.

5.4.4. O treinamento será realizado para no mínimo 5 (cinco) alunos e no máximo 10 (dez) alunos simultaneamente.

5.4.5. O treinamento deverá ser realizado por videoconferência.

5.4.6. A Contratada deverá fornecer aos participantes do treinamento os certificados de conclusão de curso contendo, no mínimo:

5.4.6.1. Nome da empresa que ministrou a capacitação;

5.4.6.2. Nome do curso;

5.4.6.3. Nome do servidor capacitado;

5.4.6.4. Data de início e término da capacitação;

5.4.6.5. Carga horária;

5.4.6.6. Conteúdo programático.

5.4.7. Os certificados deverão ser entregues no prazo de 10 (dez) dias corridos contados após o término do treinamento.

5.4.8. Ao final do treinamento, os servidores participantes efetuarão uma avaliação do conteúdo ministrado. A qualidade será medida de 1 (um) a 10 (dez) pontos em cada um dos seguintes critérios:

5.4.8.1. Pontualidade;

5.4.8.2. Didática do instrutor;

5.4.8.3. Eficiência no repasse do conteúdo;

5.4.8.4. Adequação do treinamento ao conteúdo exigido no item 5.4.1 deste Anexo;

5.4.8.5. Adequação da carga horária.

5.4.9. Caso a média das avaliações seja inferior a 7 (sete) pontos, o fornecedor deverá refazer o treinamento, após as adequações necessárias, especialmente de substituição do Instrutor, e sem qualquer custo adicional para a TRF1, sendo que esse novo treinamento também será submetido aos mesmos critérios de avaliação.

5.4.10. A realização de novo treinamento substitutivo deverá ocorrer em até 60 (sessenta) dias corridos, em data proposta pelo fornecedor e aprovada pela TRF1.

5.4.11. O fornecedor arcará com despesas de encargos tributários, bem como transporte e alimentação do instrutor.

5.5. SOLUÇÃO DE ANTIVÍRUS PARA ESTAÇÕES DE TRABALHO

5.5.1. Características gerais:

5.5.1.1. Entende-se por agente ou antivírus como sendo a ferramenta de proteção contra malwares ou vírus, termo a ser usado tanto para os componentes de proteção de estações de trabalho ou equipamentos servidores;

5.5.1.2. A Solução deverá ser baseada na arquitetura cliente/servidor, sendo composta por componente de gerência centralizada única e agentes antivírus:

5.5.1.2.1. O serviço de gerência centralizada deverá ser ofertado, preferencialmente, a partir da nuvem. Caso o fornecedor oferte serviço de gerência centralizada de solução on-premise, essa deverá ser disponibilizada por meio de appliance virtual do mesmo fabricante da solução ofertada ou a Contratada deverá realizar a instalação e configuração do(s) servidor(es) no ambiente disponibilizado, sem custo adicional para o Contratante;

5.5.1.2.2. O tráfego de dados entre os agentes e gerência centralizada deverá ocorrer através de conexão segura;

5.5.1.2.3. Os componentes da solução deverão manter compatibilidade com o ambiente tecnológico da Justiça Federal da 1ª Região - JF1, conforme descrito no item 06 deste Anexo;

5.5.1.3. A solução deverá permitir instalação dos agentes de forma remota, abrangendo todas as Seções e Subseções;

5.5.1.4. A solução deverá ser fornecida pronta para utilização imediata da JF1, não sendo permitida apresentação de qualquer procedimento que configure o desenvolvimento da solução após a contratação;

5.5.1.5. A solução deverá ser de um único fabricante, não devendo ser composta por módulos, softwares, scripts ou plug-ins de terceiros;

5.5.1.5.1. Ressalvados os casos em que a solução ofertada utilize módulos do próprio Sistema Operacional, como Firewall e recursos de proteção antimalware nativos;

5.5.1.6. A solução deverá oferecer proteção em camadas para detecção de malwares;

5.5.1.7. O fabricante deverá oferecer serviço de análise e criação de solução específica para quando for identificado um possível malware não detectado pela solução antivírus;

5.5.2. Gerenciamento centralizado:

5.5.2.1. A console de gerência centralizada deverá oferecer interface baseada em modo gráfico (GUI) acessível por software ou navegador web de forma segura (HTTPS);

5.5.2.2. Permitir o gerenciamento, controle, configuração e operação de todo parque (produtos instalados nos clientes e quaisquer outros módulos que componham a solução) de forma remota e centralizada;

5.5.2.3. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no item 06 deste Anexo;

5.5.2.4. Deverá permitir acessos simultâneos de vários usuários à console da gerência (sessões);

5.5.2.5. Deverá possuir uma base de dados centralizada para armazenamento das informações e logs dos clientes e da gerência;

5.5.2.6. Deverá permitir a criação e distribuição de políticas e tarefas remotamente para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

5.5.2.7. Deverá permitir operações de instalação, desinstalação e atualização dos módulos da solução para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

5.5.2.8. Oferecer mecanismo de comunicação (via push) entre o(s) servidor(es) e os clientes para entrega de dados e informações;

5.5.2.9. Oferecer mecanismo de comunicação (via pull) entre os clientes e o(s) servidor(es) para consulta de dados e informações de forma randômica;

5.5.2.10. A instalação ou atualização dos módulos componentes da solução, distribuição de configurações, políticas e tarefas da gerência aos clientes deve ser realizada de forma silenciosa e sem necessidade de reinicialização ou logoff do equipamento e sem necessidades de aguardar alguma ação do usuário do equipamento;

5.5.2.11. Deverá oferecer funcionalidade de execução, criação e customização de consultas às informações contidas na base de dados;

5.5.2.11.1. Deverá possibilitar a disponibilização das informações em modo de gráficos ou tabelas;

5.5.2.11.2. Deverá ser possível exportar as informações obtidas nas consultas em pelo menos um desses formatos: PDF, HTML, TXT, CSV ou Json;

5.5.2.11.3. Deverá permitir criação de alertas e notificação de eventos para administradores e usuários determinados;

5.5.2.11.4. Deverá possibilitar pesquisa no histórico de eventos;

5.5.2.11.5. Deverá permitir execução de consultas por agendamento e envio do resultado via email;

5.5.2.12. Deverá disponibilizar as seguintes consultas pré-definidas:

5.5.2.12.1. Máquinas com maior número de ocorrência de vírus e ameaças;

5.5.2.12.2. Usuários com maior número de ocorrência de vírus e ameaças;

5.5.2.12.3. Histórico de infecções nas últimas 24 horas, 7 dias e 30 dias;

5.5.2.12.4. Vírus e ameaças com maior número de registros nas últimas 24 horas, 7 dias e 30 dias;

5.5.2.12.5. Versões dos produtos instalados;

5.5.2.12.6. Versões das vacinas, quando for o caso, ou outras políticas de proteção adotadas.

5.5.2.13. Deverá permitir criação de dashboards;

5.5.2.14. Deverá permitir integração com o Active Directory da JF1 para descoberta de equipamentos ou de forma nativa na própria solução;

5.5.2.14.1. Deverá dar suporte a estrutura de florestas/domínios e subdomínios do Active Directory, refletindo a estrutura hierárquica da JF1 no Active Directory: TRF1 > Seções Judiciárias > Subseções Judiciárias.

5.5.2.15. Deverá permitir visualização ou agrupamento dos agentes instalados e gerenciados de forma a refletir a estrutura hierárquica da JF1, na forma representada no Active Directory, observando a ordem: Tribunal Regional Federal da 1ª Região - TRF1 > Seção Judiciária > Subseção Judiciária, seguindo a representação da Figura 1: Mapa Arquitetural, constante do subitem 6.4 deste Anexo;

5.5.2.16. Deverá ser capaz de distinguir e agrupar equipamentos servidores, estações de trabalho e notebooks, de forma a definir agrupamentos distintos para aplicação de regras, tarefas e políticas;

5.5.2.17. Deverá permitir que se configure diferentes políticas e tarefas para diferentes agrupamentos de computadores, seja para pontos específicos na estrutura em árvore (Seção, Subseção) como para demais grupos específicos (servidores ou estações de trabalho);

5.5.2.18. Deverá possibilitar função de herança de políticas e tarefas entre os grupos e subgrupos, com possibilidade de quebra de herança;

5.5.2.19. O acesso à console da gerência centralizada deverá ser efetuado mediante autenticação segura através de usuário cadastrado na

base de dados da solução ou através de autenticação integrada com usuários do Active Directory;

5.5.2.20. Todas as ações realizadas pelos usuários da gerência deverão ser registradas em log de auditoria, com no mínimo descrição da ação, nome do usuário, data e hora da ação realizada:

5.5.2.20.1. No caso de gerência em nuvem a solução deverá prover retenção de log por no mínimo 3 (três) meses online e possibilitar sua exportação.

5.5.2.20.2. No caso de gerência on-premise a solução deverá possibilitar criar backup da base de dados.

5.5.2.21. Deve permitir cadastro de usuários com, pelo menos, os seguintes perfis (ou equivalentes):

5.5.2.21.1. Administradores, com acesso a todas as funcionalidades da gerência e em toda a estrutura hierárquica da JF1;

5.5.2.21.2. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da JF1;

5.5.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da JF1 ou pontos específicos;

5.5.2.22. Deverá permitir instalação e desinstalação remota dos agentes antivírus, através da console de gerenciamento;

5.5.2.23. A solução deverá ser capaz de detectar e listar equipamentos conectados na rede e que não possuam a solução instalada;

5.5.2.24. Deverá identificar através da integração com o Active Directory, ou de forma nativa pela própria solução, computadores sem o agente antivírus instalado;

5.5.2.25. Deverá apresentar a funcionalidade de instalação da solução nos equipamentos detectados através da listagem de equipamentos sem o antivírus instalado ou por meio do Active Directory ou por orquestradores.

5.5.2.26. Deverá possibilitar o download de pacotes executáveis de instalação para proceder com instalação manual nos equipamentos, observado os sistemas operacionais suportados;

5.5.2.27. Deverá permitir limpeza automática de agentes inativos por determinado período de tempo, liberando as respectivas licenças;

5.5.2.28. No caso da solução em nuvem, a plataforma deverá ser certificada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes);

5.5.2.29. Deverá ser possível criação de políticas para distribuição de atualizações para o parque gerenciado com periodicidade mínima diária;

5.5.2.30. Deverá ser possível criação de políticas para distribuição de atualizações e vacinas para o parque gerenciado com periodicidade mínima diária;

5.5.2.31. Deverá permitir configuração alternativa para permitir que o agente busque atualização na nuvem do fabricante quando estiver fora do escopo da gerência centralizada;

5.5.2.32. As atualizações deverão ser do tipo incremental;

5.5.2.33. Deverá permitir distribuição de versões diferentes da solução para diferentes grupos de equipamentos;

5.5.2.33.1. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, restaurar e excluir;

5.5.2.34. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, limpar e excluir;

5.5.2.35. Deverá possibilitar restauração manual de arquivos quarentenados;

5.5.2.36. Deverá permitir criar listas de exclusões ou exceções para determinados aplicativos ou diretórios e subdiretórios;

5.5.2.37. Deverá utilizar os recursos locais de forma otimizada, sem impacto no desempenho do endpoint, ou possibilitar a configuração de baixo uso de recurso do dispositivo nas operações do agente antivírus;

5.5.2.38. Deverá permitir criação de políticas para bloqueio de dispositivos de armazenamento externos;

5.5.2.39. Deverá possibilitar extração de informações sobre dispositivos bloqueados, contendo no mínimo data e hora do ocorrido, equipamento onde o bloqueio ocorreu, rótulo do dispositivo bloqueado e usuário do sistema operacional logado durante o bloqueio;

5.5.2.40. Deverá fornecer solução Sandbox, em nuvem ou on-premise, para análise de malwares e mecanismo de reputação de softwares.

5.5.2.40.1. Em caso de fornecimento do Sandbox on-premise a Contratada deverá instalar e fornecer todos os recursos logísticos e de infraestrutura necessários para implantação do equipamento no ambiente do Contratante, a exemplo de alimentação elétrica, cabeamento, sem custo adicional.

5.5.2.40.2. As funcionalidades do serviço de Sandbox deverão ser integrados na gerência centralizada;

5.5.2.41. Deverá possibilitar aplicar bloqueios e respostas para ameaças detectadas e analisadas pelo serviço de Sandbox em todo o parque;

5.5.2.42. Deverá apresentar interface para investigação usando funcionalidades de Detecção e Resposta, sendo possível tomar ações para os equipamentos em análise;

5.5.3. Serviço de Desinstalação

5.5.3.1. A desinstalação do parque atual existente na JF1 deverá ser efetuada pela CONTRATADA;

5.5.3.2. A CONTRATANTE deverá fornecer as credenciais necessárias para a execução da desinstalação, como usuário com privilégio.

5.5.3.3. A estratégia a ser adotada na execução da desinstalação será previamente acordada entre o CONTRATANTE e a CONTRATADA.

5.5.3.4. A desinstalação da ferramenta existente deverá ocorrer de forma silenciosa para o usuário, sem necessitar de reboot do equipamento e sem solicitar ações do usuário da estação/servidor;

5.5.3.4.1. Em casos específicos onde seja necessário reboot, deverá ser informado para a CONTRANTE para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar;

5.5.3.5. O equipamento onde for instalado a nova solução deverá estar LIMPA e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações em que mais de 1 solução além da vigente por este certame estejam instaladas no equipamento ao mesmo tempo;

5.5.3.6. Problemas na execução da desinstalação do agente deverão ser imediatamente comunicadas a CONTRATANTE;

5.5.4. Serviço de instalação e configuração

5.5.4.1. A instalação deverá ocorrer em todo o âmbito da JF1;

5.5.4.2. A instalação do agente deverá pressupor desinstalação da solução anterior;

5.5.4.3. A instalação do agente deverá ser imperceptível para o usuário, de forma a não aparecer pop-ups, mensagens, caixas de diálogos solicitando ação de usuário e nem janelas modais, de forma a interromper de qualquer forma o usuário;

5.5.4.4. Os serviços de instalação devem compreender a configuração da gerência centralizada em nuvem ou a configuração dos equipamentos servidores virtuais para os componentes da solução on-premise, incluindo appliance virtual da gerência centralizada, banco de dados da solução e demais componentes a serem utilizados pela solução de gerência;

5.5.4.5. Deverá possibilitar a instalação dos componentes da solução de forma a refletir a estrutura hierárquica da JF1, observando a ordem: TRF1 > Seção Judiciária > Subseção Judiciária e o gráfico arquitetural Figura 1: Mapa Arquitetural, constante do subitem 6.4 deste Anexo;

5.5.4.6. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as Seções e Subseções;

5.5.4.7. Deve permitir que se instale os agentes individualmente por computador ou em lote, para vários computadores;

5.5.4.8. A interoperabilidade entre os componentes da solução deverá ser configurada por políticas na gerência e utilizando protocolos seguros;

5.5.4.9. Deverá permitir que se programe através de políticas o agendamento da distribuição dos itens atualizados na gerência centralizada para os repositórios;

5.5.4.10. Ao final do processo de instalação a CONTRATADA deverá fornecer os seguintes relatórios:

5.5.4.10.1. Relação de todos os computadores contendo antivírus instalado, com no mínimo as seguintes informações, agrupados por localidade – Subseção/Seção/TRF1;

5.5.4.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção/Seção/TRF1, contendo no mínimo:

5.5.4.10.2.1. Versão de cada módulo da solução instalado;

5.5.4.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

5.5.4.10.2.3. Versão de demais bibliotecas ou catálogos que compõem a solução instalado;

5.5.4.10.2.4. Os relatórios serão utilizados para avaliar conformidade da prestação do serviço de instalação;

5.5.4.10.2.5. Serão comparados com o quantitativo de máquinas ativas na JF1, utilizando a seguinte fórmula para apurar o índice de instalação:

5.5.4.10.2.5.1. IND – Índice de instalação;

5.5.4.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

5.5.4.10.2.5.3. QLA – Quantidade licenças adquiridas;

5.5.4.10.2.5.4. Será dado aceite da solução quando o resultado da instalação IND possua valor igual ou superior a 0.8 – IND >= 0.8;

5.5.5. Solução de antivírus para estações de trabalho

5.5.5.1. Deverá ser compatível com as seguintes tecnologias de sistema operacional, no mínimo:

5.5.5.1.1. Windows 8.1;

5.5.5.1.2. Windows 10;

5.5.5.1.3. Linux CentOS;

5.5.5.1.4. Linux Debian;

5.5.5.2. Deverá proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares;

5.5.5.3. A solução e todos os seus componentes deverão funcionar como um agente composto por um executável único que será instalado na estação de trabalho, podendo encapsular os diversos módulos que compõe a solução;

5.5.5.3.1. Caso a solução utilize de recursos de segurança nativos do Sistema Operacional, os mesmos serão considerados como módulos do agente único utilizado;

5.5.5.3.2. O módulo EDR poderá ser disponibilizado através de um executável ou módulo separado ao da solução de antivírus;

5.5.5.4. Deverá ser capaz de reconhecer ataques e ações maliciosas por assinatura, por análise heurística ou por machine learning;

5.5.5.5. Soluções que usem somente método de detecção por assinatura não serão aceitas;

5.5.5.6. Deverá possuir mecanismo de análise comportamental;

5.5.5.7. Deverá ser capaz de proteger ataques provenientes de malwares;

5.5.5.8. Deverá ser capaz de realizar proteção contra ameaças mesmo estando o dispositivo não conectado à internet;

5.5.5.9. Quando o equipamento estiver fora da cobertura da gerência centralizada deverá ser capaz de buscar atualizações na internet, na nuvem do fabricante;

5.5.5.10. Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo e hash do arquivo;

5.5.5.11. Deverá ser capaz de detectar, alertar e prevenir quando for detectado alguma ameaça;

5.5.5.12. Deverá ser capaz de prover proteção contra-ataques que explorem vulnerabilidades do sistema operacional do host, de acordo com o estabelecido no item 5.5.5.1 deste Anexo;

5.5.5.13. Deverá possuir proteção contra BOTs e variantes;

5.5.5.14. Deverá efetuar proteção permanente e em tempo real dos processos em memória;

5.5.5.14.1. Processos suspeitos deverão ser bloqueados;

5.5.5.15. Deverá possuir mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados e contra ameaças avançadas e persistentes, que não são detectadas pelos métodos convencionais de antivírus;

5.5.5.16. Deverá ser capaz de detectar variações de malwares geradas em memória principal;

5.5.5.17. Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial do tipo Machine Learning;

5.5.5.18. Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação;

5.5.5.19. Deverá oferecer proteção contra-ataques de 0Day (dia zero);

5.5.5.20. Deverá oferecer proteção contra Ransomwares, com capacidade de avaliar processos criptográficos em execução no sistema,

exclusão de backups, número alto de operações de I/O no sistema de arquivos;

5.5.5.21. Deverá informar o nome ou endereço IP da origem do ataque ou infecção;

5.5.5.22. Deverá oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código Hash do executável, caminho e nome do aplicativo malicioso;

5.5.5.23. Deverá oferecer proteção contra vírus de macro e por scripts variados, incluindo bash e powershell;

5.5.5.24. Deverá oferecer mecanismo de bloqueio baseado em análise realizada pela central de inteligência do fabricante oriundo da nuvem;

5.5.5.25. Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas;

5.5.5.26. Deverá possibilitar visualizar toda a cadeia de ataque, inclusive os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros;

5.5.5.27. Deverá oferecer proteção para alterações suspeitas de registro;

5.5.5.28. Deverá prover mecanismos para criação proteções personalizadas para detecção;

5.5.5.29. Deverá oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção);

5.5.5.30. Deverá oferecer proteção contra-ataques direcionados;

5.5.5.31. Deverá gerar log local assim como enviá-los para a gerência;

5.5.5.32. Deverá permitir inclusão de exceções aplicações e caminhos;

5.5.5.33. A solução deverá oferecer proteção para ameaças em execução:

5.5.5.33.1. Na memória principal (RAM);

5.5.5.33.2. Em arquivos;

5.5.5.33.3. No tráfego de rede;

5.5.5.33.4. Em dados provenientes de browsers de navegação web (downloads, scripts, etc);

5.5.5.33.5. Em arquivos compactados (formatos zip, exe, cab, rar, etc);

5.5.5.33.6. Em processos de inicialização automática;

5.5.5.33.7. Em serviços criados/modificados;

5.5.5.34. Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados;

5.5.5.35. Deverá permitir bloqueio de alterações nas configurações do antivírus por parte do usuário, sendo permitido apenas por alterações de políticas ou mediante inserção de senha/password, definidos na gerência;

5.5.5.36. Deverá possibilitar a criação de lista de aplicações confiáveis (lista de exceções), a partir da gerência centralizada, para eliminação de detecções do tipo falso positivo;

5.5.5.36.1. Deverá oferecer a possibilidade de editar esta lista, com inclusão e remoção de aplicativos;

5.5.5.37. Deverá possuir a capacidade de detectar antivírus de outros fabricantes que possam acarretar incompatibilidade;

5.5.5.38. Deverá impedir execução e instalação de aplicativos cujo comportamento seja suspeito ou que constem na lista de aplicativos inseridos na gerência centralizada;

5.5.5.39. Deverá detectar e proteger em tempo real o computador contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de páginas da web e scripts em linguagens tais como javascript, vbscript, activex, etc;

5.5.5.40. Deverá oferecer mecanismo de controle de dispositivos externos;

5.5.5.41. A administração das regras da funcionalidade para controle mecanismos externos deverá ser realizada a partir da gerência centralizada;

5.5.5.42. O mecanismo de controle de dispositivos externos deverá possibilitar monitorar e bloquear dispositivos a partir de regras e políticas estabelecidas na gerencia centralizada, para no mínimo:

5.5.5.42.1. Dispositivos de rede externos (wifi portátil, dispositivos de dados móveis);

5.5.5.42.2. Transferências de dados para dispositivos mobile.;

5.5.5.42.3. Transferências de dados para dispositivos de armazenamento externos;

5.5.5.42.4. Possibilitar ações de bloqueio na execução de arquivos em transferência através de browsers e clientes de e-mail.

5.5.5.43. Deve oferecer ou executar uma das seguintes opções de ações corretivas para programas maliciosos detectados: bloquear o objeto, executar a limpeza da ameaça e executar ação de quarentena;

5.5.5.44. Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma que não seja perceptível aos seus usuários e nem influenciem negativamente no rendimento de aplicações em servidores;

5.5.5.45. No mínimo as seguintes ocorrências deverão ser registradas em arquivo de log local ou enviadas para a gerência centralizada:

5.5.5.45.1. Atualização de engine e/ou repositório de vacinas.

5.5.5.45.2. Recebimento de políticas e tarefas da gerência;

5.5.5.45.3. Inicialização e finalização de varreduras, agendadas ou manuais, ou quando realizada por meio de análise dos processos em tempo real baseado em machine learning;

5.5.5.45.4. Detecção de alguma ameaça, registrando no mínimo as seguintes informações:

5.5.5.45.4.1. Nome da ameaça;

5.5.5.45.4.2. Tipo da ameaça;

5.5.5.45.4.3. Arquivo ou local infectado;

5.5.5.45.4.4. Data e hora da detecção;

5.5.5.45.4.5. Mecanismo que gerou a detecção;

5.5.5.45.4.6. Nome da máquina/endereço IP;

5.5.5.45.4.7. Ação realizada;

5.5.5.45.4.8. Usuário logado no sistema;

5.5.5.46. Deverá buscar por itens de atualização nos repositórios, configurado pela gerência, de acordo com topologia e políticas especificadas;

5.5.5.47. Deverá possibilitar mais de uma versão da ferramenta e seus insumos, para que em casos de incompatibilidades decorrentes de atualizações, seja possível reinstalar versões anteriores estáveis ou instalar

versões novas em grupos específicos, para fins de testes de compatibilidade antes de instalação em todo parque;

5.5.5.48. Deverá fornecer informações do status do agente e de seus componentes, através da gerência com informações atualizadas com delay máximo de 5 minutos;

5.5.5.49. Deve ser disponibilizado nos idiomas português, preferencialmente, ou inglês;

5.5.6. Garantia e atualização das licenças, para estações de trabalho

5.5.6.1. A garantia técnica deverá ser contratada junto ao fabricante da solução, e sua vigência não poderá ser inferior ao período de 60 (sessenta) meses, contados a partir da aceitação definitiva da solução;

5.5.6.2. O atendimento do serviço de suporte técnico da garantia, deverá ser feito por intermédio da CONTRATADA ou diretamente com a fabricante através de portal específico para fins de suporte ou por e-mail;

5.5.6.3. A garantia técnica deverá ser acionada nas situações específicas onde a CONTRATADA não conseguir solução para o problema ou quando o problema for detectado em relação aos elementos da solução contratada, tais como bugs ou algum mal funcionamento;

5.5.6.4. A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução;

5.5.6.5. As atualizações deverão ser fornecidas independente de solicitação da CONTRATANTE.

5.5.6.6. Deverão ser providas atualizações das listas de definições de vírus e demais insumos para funcionamento atualizado da solução, de acordo com o mercado;

5.5.6.7. Deverá permitir atualizações da engine do agente (software), assim como da base de dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução;

5.5.6.8. A garantia técnica contempla suporte técnico do fabricante, serviços de manutenções e atualizações da solução antivírus, base de dados de vacinas, bem como disponibilização de:

5.5.6.8.1. Solução de problemas que afetem elementos da solução, incluindo os softwares, atualizações e instalação, evoluções, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;

5.5.6.8.2. Manuais dos produtos e serviços ofertados, base de conhecimento para soluções conhecidas, canal de comunicação, esclarecimento de dúvidas e quaisquer outras informações solicitadas pela CONTRATANTE:

5.5.6.8.2.1. As informações prestadas deverão ser disponibilizadas preferencialmente no idioma Português do Brasil ou na falta deste, obrigatoriamente no idioma em Inglês;

5.5.6.8.3. Novas versões da solução lançadas pelo fabricante e lançamento de novos softwares em substituição da solução contratada, em caso de descontinuação do software fornecido.

5.5.6.9. Os serviços descritos neste item deverão ser prestados mediante abertura de chamado pela CONTRATANTE ou pela CONTRATADA, diretamente no portal de comunicação e suporte do fabricante, realizado por meio de e-mail e site de helpdesk;

5.5.6.10. A garantia deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia.

5.6. SOLUÇÃO DE ANTIVIRUS PARA SERVIDORES

5.6.1. Características gerais:

5.6.1.1. Entende-se por agente ou antivírus como sendo a ferramenta de proteção contra malwares ou vírus, termo a ser usado tanto para os componentes de proteção de estações de trabalho ou equipamentos servidores;

5.6.1.2. A Solução deverá ser baseada na arquitetura cliente/servidor, sendo composta por componente de gerência centralizada e agentes antivírus:

5.6.1.2.1. O serviço de gerência centralizada deverá ser ofertado, preferencialmente, a partir da nuvem. Caso o fornecedor oferte serviço de gerência centralizada de solução on-premise, essa deverá ser disponibilizada por meio de appliance virtual do mesmo fabricante da solução ofertada ou a Contratada deverá realizar a instalação e configuração do(s) servidor(es) no ambiente disponibilizado, sem custo adicional para o Contratante;

5.6.1.2.2. O tráfego de dados entre os agentes e gerência centralizada deverá ocorrer através de conexão segura;

5.6.1.2.3. Os componentes da solução deverão manter compatibilidade com o ambiente tecnológico da Justiça Federal da 1ª Região - JF1, conforme descrito no item 06 deste Anexo;

5.6.1.3. A solução deverá permitir instalação dos agentes de forma remota, abrangendo todas as Seções e Subseções;

5.6.1.4. A solução deverá ser fornecida pronta para utilização imediata da JF1, não sendo permitida apresentação de qualquer procedimento que configure o desenvolvimento da solução após a contratação;

5.6.1.5. A solução deverá ser de um único fabricante, não devendo ser composta por módulos, softwares, scripts ou plug-ins de terceiros;

5.6.1.5.1. Ressalvados os casos em que a solução ofertada utilize módulos do próprio Sistema Operacional, como Firewall e recursos de proteção antimalware nativos;

5.6.1.6. A solução deverá oferecer proteção em camadas para detecção de malwares;

5.6.1.7. O fabricante deverá oferecer serviço de análise e criação de solução específica para quando for identificado um possível malware não detectado pela solução antivírus;

5.6.2. Gerenciamento centralizado:

5.6.2.1. A console de gerência centralizada deverá oferecer interface baseada em modo gráfico (GUI) acessível por software ou navegador web de forma segura (HTTPS);

5.6.2.2. Permitir o gerenciamento, controle, configuração e operação de todo parque (produtos instalados nos clientes e quaisquer outros módulos que componham a solução) de forma remota e centralizada;

5.6.2.3. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no item 06 deste Anexo;

5.6.2.4. Deverá permitir acessos simultâneos de vários usuários à console da gerência (sessões);

5.6.2.5. Deverá possuir uma base de dados centralizada para armazenamento das informações e logs dos clientes e da gerência;

5.6.2.6. Deverá permitir a criação e distribuição de políticas e tarefas remotamente para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

5.6.2.7. Deverá permitir operações de instalação, desinstalação e atualização dos módulos da solução para todo agrupamento de itens gerenciados, grupos específicos ou itens individuais através da console de gerência;

5.6.2.8. Oferecer mecanismo de comunicação (via push) entre o(s) servidor(es) e os clientes para entrega de dados e informações;

5.6.2.9. Oferecer mecanismo de comunicação (via pull) entre os clientes e o(s) servidor(es) para consulta de dados e informações de forma randômica;

5.6.2.10. A instalação ou atualização dos módulos componentes da solução, distribuição de configurações, políticas e tarefas da gerência aos clientes deve ser realizada de forma silenciosa e sem necessidade de reinicialização ou logoff do equipamento e sem necessidades de aguardar alguma ação do usuário do equipamento;

5.6.2.11. Deverá oferecer funcionalidade de execução, criação e customização de consultas às informações contidas na base de dados;

5.6.2.11.1. Deverá possibilitar a disponibilização das informações em modo de gráficos ou tabelas;

5.6.2.11.2. Deverá ser possível exportar as informações obtidas nas consultas em pelo menos um desses formatos: PDF, HTML, TXT, CSV ou Json;

5.6.2.11.3. Deverá permitir criação de alertas e notificação de eventos para administradores e usuários determinados;

5.6.2.11.4. Deverá possibilitar pesquisa no histórico de eventos;

5.6.2.11.5. Deverá permitir execução de consultas por agendamento e envio do resultado via email;

5.6.2.12. Deverá disponibilizar as seguintes consultas pré-definidas:

5.6.2.12.1. Máquinas com maior número de ocorrência de vírus e ameaças;

5.6.2.12.2. Usuários com maior número de ocorrência de vírus e ameaças;

5.6.2.12.3. Histórico de infecções nas últimas 24 horas, 7 dias e 30 dias;

5.6.2.12.4. Vírus e ameaças com maior número de registros nas últimas 24 horas, 7 dias e 30 dias;

5.6.2.12.5. Versões dos produtos instalados;

5.6.2.12.6. Versões das vacinas, quando for o caso, ou outras políticas de proteção adotadas.

5.6.2.13. Deverá permitir criação de dashboards;

5.6.2.14. Deverá permitir integração com o Active Directory da JF1 para descoberta de equipamentos ou de forma nativa na própria solução;

5.6.2.14.1. Deverá dar suporte a estrutura de florestas/domínios e subdomínios do Active Directory, refletindo a estrutura hierárquica da JF1 no Active Directory: TRF1 > Seções Judiciárias > Subseções Judiciárias

5.6.2.15. Deverá permitir visualização ou agrupamento dos agentes instalados e gerenciados de forma a refletir a estrutura hierárquica da JF1, na forma representada no Active Directory, observando a ordem: Tribunal Regional Federal da 1ª Região - TRF1 > Seção Judiciária > Subseção Judiciária, seguindo a representação da Figura 1: Mapa Arquitetural, constante do subitem 6.4 deste Anexo;

5.6.2.16. Deverá ser capaz de distinguir e agrupar equipamentos servidores, estações de trabalho e notebooks, de forma a definir agrupamentos distintos para aplicação de regras, tarefas e políticas;

5.6.2.17. Deverá permitir que se configure diferentes políticas e tarefas para diferentes agrupamentos de computadores, seja para pontos específicos na estrutura em árvore (Seção, Subseção) como para demais grupos específicos (servidores ou estações de trabalho);

5.6.2.18. Deverá possibilitar função de herança de políticas e tarefas entre os grupos e subgrupos, com possibilidade de quebra de herança;

5.6.2.19. O acesso à console da gerência centralizada deverá ser efetuado mediante autenticação segura através de usuário cadastrado na base de dados da solução ou através de autenticação integrada com usuários do Active Directory;

5.6.2.20. Todas as ações realizadas pelos usuários da gerência deverão ser registradas em log de auditoria, com no mínimo descrição da ação, nome do usuário, data e hora da ação realizada:

5.6.2.20.1. No caso de gerência em nuvem a solução deverá prover retenção de log por no mínimo 3 (três) meses online e possibilitar sua exportação.

5.6.2.20.2. No caso de gerência on-premise a solução deverá possibilitar criar backup da base de dados.

5.6.2.21. Deve permitir cadastro de usuários com, pelo menos, os seguintes perfis (ou equivalentes):

5.6.2.21.1. Administradores, com acesso a todas as funcionalidades da gerência e em toda a estrutura hierárquica da JF1;

5.6.2.21.2. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da JF1;

5.6.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da JF1 ou pontos específicos;

5.6.2.22. Deverá permitir instalação e desinstalação remota dos agentes antivírus, através da console de gerenciamento;

5.6.2.23. A solução deverá ser capaz de detectar e listar equipamentos conectados na rede e que não possuam a solução instalada;

5.6.2.24. Deverá identificar através da integração com o Active Directory, ou de forma nativa pela própria solução, computadores sem o agente antivírus instalado;

5.6.2.25. Deverá apresentar a funcionalidade de instalação da solução nos equipamentos detectados através da listagem de equipamentos sem o antivírus instalado ou por meio do Active Directory ou por orquestradores.

5.6.2.26. Deverá possibilitar o download de pacotes executáveis de instalação para proceder com instalação manual nos equipamentos, observado os sistemas operacionais suportados;

5.6.2.27. Deverá permitir limpeza automática de agentes inativos por determinado período de tempo, liberando as respectivas licenças;

5.6.2.28. No caso da solução em nuvem, a plataforma deverá ser certificada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes);

5.6.2.29. Deverá ser possível criação de políticas para distribuição de atualizações para o parque gerenciado com periodicidade mínima diária;

5.6.2.30. Deverá ser possível criação de políticas para distribuição de atualizações e vacinas para o parque gerenciado com periodicidade mínima diária;

5.6.2.31. Deverá permitir configuração alternativa para permitir que o agente busque atualização na nuvem do fabricante quando estiver fora do escopo da gerência centralizada;

5.6.2.32. As atualizações deverão ser do tipo incremental;

5.6.2.33. Deverá permitir distribuição de versões diferentes da solução para diferentes grupos de equipamentos;

5.6.2.33.1. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, restaurar e excluir;

5.6.2.34. Deverá permitir determinar ações para arquivos infectados, como deixar em quarentena, limpar e excluir;

5.6.2.35. Deverá possibilitar restauração manual de arquivos quarentenados;

5.6.2.36. Deverá permitir criar listas de exclusões ou exceções para determinados aplicativos ou diretórios e subdiretórios;

5.6.2.37. Deverá utilizar os recursos locais de forma otimizada, sem impacto no desempenho do endpoint, ou possibilitar a configuração de baixo uso de recurso do dispositivo nas operações do agente antivírus;

5.6.2.38. Deverá permitir criação de políticas para bloqueio de dispositivos de armazenamento externos;

5.6.2.39. Deverá possibilitar extração de informações sobre dispositivos bloqueados, contendo no mínimo data e hora do ocorrido, equipamento onde o bloqueio ocorreu, rótulo do dispositivo bloqueado e usuário do sistema operacional logado durante o bloqueio;

5.6.2.40. Deverá fornecer solução Sandbox, em nuvem ou on-premise, para análise de malwares e mecanismo de reputação de softwares.

5.6.2.40.1. Em caso de fornecimento do Sandbox on-premise a Contratada deverá instalar e fornecer todos os recursos logísticos e de infraestrutura necessários para implantação do equipamento no ambiente do Contratante, a exemplo de alimentação elétrica, cabeamento, sem custo adicional.

5.6.2.40.2. As funcionalidades do serviço de Sandbox deverão ser integrados na gerência centralizada;

5.6.2.41. Deverá possibilitar aplicar bloqueios e respostas para ameaças detectadas e analisadas pelo serviço de Sandbox em todo o parque;

5.6.2.42. Deverá apresentar interface para investigação usando funcionalidades de Detecção e Resposta, sendo possível tomar ações para os equipamentos em análise;

5.6.3. Serviço de Desinstalação

5.6.3.1. A desinstalação do parque atual existente na JF1 deverá ser efetuada pela CONTRATADA;

5.6.3.2. A CONTRATANTE deverá fornecer as credenciais necessárias para a execução da desinstalação, como usuário com privilégio.

5.6.3.3. A estratégia a ser adotada na execução da desinstalação será previamente acordada entre o CONTRATANTE e a CONTRATADA.

5.6.3.4. A desinstalação da ferramenta existente deverá ocorrer de forma silenciosa para o usuário, sem necessitar de reboot do equipamento e sem solicitar ações do usuário da estação/servidor;

5.6.3.4.1. Em casos específicos onde seja necessário reboot, deverá ser informado para a CONTRANTE para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar;

5.6.3.5. O equipamento onde for instalado a nova solução deverá estar LIMPA e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações em que mais de 1 solução além da vigente por este certame estejam instaladas no equipamento ao mesmo tempo;

5.6.3.6. Problemas na execução da desinstalação do agente deverão ser imediatamente comunicadas a CONTRATANTE;

5.6.4. Serviço de instalação e configuração

5.6.4.1. A instalação deverá ocorrer em todo o âmbito da JF1;

5.6.4.2. A instalação do agente deverá pressupor desinstalação da solução anterior;

5.6.4.3. A instalação do agente deverá ser imperceptível para o usuário, de forma a não aparecer pop-ups, mensagens, caixas de diálogos solicitando ação de usuário e nem janelas modais, de forma a interromper de qualquer forma o usuário;

5.6.4.4. Os serviços de instalação devem compreender a configuração da gerência centralizada em nuvem ou a configuração dos equipamentos servidores virtuais para os componentes da solução on-premise, incluindo

appliance virtual da gerência centralizada, banco de dados da solução e demais componentes a serem utilizados pela solução de gerência;

5.6.4.5. Deverá possibilitar a instalação dos componentes da solução de forma a refletir a estrutura hierárquica da JF1, observando a ordem: TRF1 > Seção Judiciária > Subseção Judiciária e o gráfico arquitetural Figura 1: Mapa Arquitetural, constante do subitem 6.4 deste Anexo;

5.6.4.6. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as Seções e Subseções;

5.6.4.7. Deve permitir que se instale os agentes individualmente por computador ou em lote, para vários computadores;

5.6.4.8. A interoperabilidade entre os componentes da solução deverá ser configurada por políticas na gerência e utilizando protocolos seguros;

5.6.4.9. Deverá permitir que se programe através de políticas o agendamento da distribuição dos itens atualizados na gerência centralizada para os repositórios;

5.6.4.10. Ao final do processo de instalação a CONTRATADA deverá fornecer os seguintes relatórios:

5.6.4.10.1. Relação de todos os computadores contendo antivírus instalado, com no mínimo as seguintes informações, agrupados por localidade – Subseção/Seção/TRF1;

5.6.4.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção/Seção/TRF1, contendo no mínimo:

5.6.4.10.2.1. Versão de cada módulo da solução instalado;

5.6.4.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

5.6.4.10.2.3. Versão de demais bibliotecas ou catálogos que compõem a solução instalado;

5.6.4.10.2.4. Os relatórios serão utilizados para avaliar conformidade da prestação do serviço de instalação;

5.6.4.10.2.5. Serão comparados com o quantitativo de máquinas ativas na JF1, utilizando a seguinte fórmula para apurar o índice de instalação:

5.6.4.10.2.5.1. IND – Índice de instalação;

5.6.4.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

5.6.4.10.2.5.3. QLA – Quantidade licenças adquiridas;

5.6.4.10.2.5.4. Será dado aceite da solução quando o resultado da instalação IND possua valor igual ou superior a 0.8 – IND >= 0.8;

5.6.5. Solução de antivírus para equipamentos servidores

5.6.5.1. Deverá ser compatível com as seguintes tecnologias de sistema operacional, no mínimo:

5.6.5.1.1. Windows Server 2012;

5.6.5.1.2. Windows Server 2016;

5.6.5.1.3. Windows Server 2019 e posteriores;

5.6.5.1.4. Linux CentOS;

5.6.5.1.5. Linux Debian;

5.6.5.1.6. Linux Red Hat;

5.6.5.2. Deverá proporcionar proteção contra ameaças, tais como vírus, ransomwares, trojans, spywares, worms, keylogers, dentre outros malwares;

5.6.5.3. A solução e todos os seus componentes deverão funcionar como um agente composto por um executável único que será instalado na estação de trabalho, podendo encapsular os diversos módulos que compõe a solução;

5.6.5.3.1. Caso a solução utilize de recursos de segurança nativos do Sistema Operacional, os mesmos serão considerados como módulos do agente único utilizado;

5.6.5.4. Deverá ser capaz de reconhecer ataques e ações maliciosas por assinatura, por análise heurística ou por machine learning.

5.6.5.5. Soluções que usem somente método de detecção por assinatura não serão aceitas;

5.6.5.6. Deverá possuir mecanismo de análise comportamental;

5.6.5.7. Deverá ser capaz de proteger ataques provenientes de malwares;

5.6.5.8. Deverá ser capaz de realizar proteção contra ameaças mesmo estando o dispositivo não conectado à internet;

5.6.5.9. Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo, caminho do aplicativo e hash do arquivo;

5.6.5.10. Deverá ser capaz de detectar, alertar e prevenir quando for detectado alguma ameaça;

5.6.5.11. Deverá ser capaz de prover proteção contra ataques que explorem vulnerabilidades do sistema operacional do host, de acordo com o estabelecido no item 5.6.5.1 deste Anexo;

5.6.5.12. Deverá possuir proteção contra BOTs e variantes;

5.6.5.13. Deverá efetuar proteção permanente e em tempo real dos processos em memória;

5.6.5.13.1. Processos suspeitos deverão ser bloqueados;

5.6.5.14. Deverá possuir mecanismos de análise avançada para proteção e remediação de vírus de código polimorfos, ofuscados, criptografados e contra ameaças avançadas e persistentes, que não são detectadas pelos métodos convencionais de antivírus;

5.6.5.15. Deverá ser capaz de detectar variações de malwares geradas em memória principal;

5.6.5.16. Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial do tipo Machine Learning;

5.6.5.17. Em casos de aplicações com comportamento malicioso detectado, deverá efetuar bloqueios de processos e efetuar isolamento de comunicação;

5.6.5.18. Deverá oferecer proteção contra ataques de 0Day (dia zero);

5.6.5.19. Deverá oferecer proteção contra Ransomwares, com capacidade de avaliar processos criptográficos em execução no sistema, exclusão de backups, número alto de operações de I/O no sistema de arquivos;

5.6.5.20. Deverá informar o nome ou endereço IP da origem do ataque ou infecção;

5.6.5.21. Deverá ter a capacidade de bloquear ataques direcionados a aplicações em execução no servidor através de funcionalidade de proteção contra vulnerabilidades conhecidas e catalogadas através de CVE ou catálogo próprio, tanto para o sistema operacional quanto para aplicações instaladas no servidor;

5.6.5.21.1. O mecanismo deverá proteger no mínimo os seguintes softwares de terceiros: Apache, Tomcat, JBoss, Microsft IIS, SQL Server, PostgreSQL, Banco de Dados Oracle, MySQL e variantes, Wordpress, Joomla, Adobe entre outros;

5.6.5.22. Em caso de ataque a solução deverá detectar comportamentos maliciosos da aplicação web;

5.6.5.23. Para sistemas operacionais windows a solução deverá gerenciar o seu Firewall ou possuir Firewall bidirecional com detecção e proteção contra intrusões e ataques.

5.6.5.23.1. Firewall deverá possibilitar ações como permitir e bloquear: portas, range de portas, IPs, range de IPs e redes;

5.6.5.23.2. Deverá ser possível aplicar regras de permitir todo tráfego ou bloquear todo tráfego;

5.6.5.24. Deverá oferecer funcionalidade de controle de aplicações, identificando aplicações no mínimo pelo código Hash do executável, caminho e nome do aplicativo malicioso;

5.6.5.25. Deverá oferecer proteção contra vírus de macro e por scripts variados, incluindo bash e powershell;

5.6.5.26. Deverá oferecer mecanismo de bloqueio baseado em análise realizada pela central de inteligência do fabricante oriundo na nuvem;

5.6.5.27. Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas

5.6.5.28. Deverá possibilitar visualizar toda a cadeia de ataque, inclusive os processos e aplicativos executados, arquivos e registros utilizados, endereços acessados, dentre outros;

5.6.5.29. Deverá oferecer proteção para alterações suspeitas de registro;

5.6.5.30. Deverá prover mecanismos para criação proteções personalizadas para detecção;

5.6.5.31. Deverá oferecer proteção contra processos que tentem alterar ou manipular indevidamente os componentes instalados e em execução do antivírus (autoproteção);

5.6.5.32. Deverá oferecer proteção contra ataques direcionados;

5.6.5.33. Deverá gerar log local assim como envia-los para a gerência, ou enviar logs em tempo real para a gerência centralizada;

5.6.5.34. Deverá permitir inclusão de exceções aplicações e caminhos;

5.6.5.35. A solução deverá oferecer proteção para ameaças em execução:

5.6.5.35.1. Na memória principal (RAM);

5.6.5.35.2. Em arquivos;

5.6.5.35.3. No tráfego de rede;

5.6.5.35.4. Em dados provenientes de browsers de navegação web (downloads, scripts, etc);

5.6.5.35.5. Em arquivos compactados (formatos zip, exe, cab, rar, etc);

5.6.5.35.6. Em processos de inicialização automática;

5.6.5.35.7. Em serviços criados/modificados;

5.6.5.36. Solução deverá efetuar a proteção permanente, em tempo real, quando arquivos forem acessados, lidos, gravados, alterados ou renomeados;

5.6.5.37. Deverá possibilitar a criação de lista de aplicações confiáveis (lista de exceções), a partir da gerencia centralizada, para eliminação de detecções do tipo falso positivo;

5.6.5.37.1. Deverá oferecer a possibilidade de editar esta lista, com inclusão e remoção de aplicativos;

5.6.5.38. Deverá possuir a capacidade de detectar antivírus de outros fabricantes que possam acarretar em incompatibilidade;

5.6.5.39. Deverá impedir execução e instalação de aplicativos cujo comportamento seja suspeito ou que constem na lista de aplicativos inseridos na gerência centralizada;

5.6.5.40. Deverá detectar e proteger em tempo real o computador contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de páginas da web e scripts em linguagens tais como javascript, vbscript, activex, etc;

5.6.5.41. Deve oferecer ou executar uma das seguintes opções de ações corretivas para programas maliciosos detectados: bloquear o objeto, executar a limpeza da ameaça e executar ação de quarentena;

5.6.5.42. Os mecanismos de proteção deverão ser executados sem comprometer o desempenho dos computadores, de forma a não influenciar negativamente no rendimento de aplicações em servidores;

5.6.5.43. No mínimo as seguintes ocorrências deverão ser registradas em arquivo de log local ou enviadas para a gerência centralizada:

5.6.5.43.1. Atualização de engine e/ou repositório de vacinas.

5.6.5.43.2. Recebimento de políticas e tarefas da gerência;

5.6.5.43.3. Inicialização e finalização de varreduras, agendadas ou manuais, ou quando realizada por meio de análise dos processos em tempo real baseado em machine learning;

5.6.5.43.4. Detecção de alguma ameaça, registrando no mínimo as seguintes informações:

5.6.5.43.4.1. Nome da ameaça;

5.6.5.43.4.2. Tipo da ameaça;

5.6.5.43.4.3. Arquivo ou local infectado;

5.6.5.43.4.4. Data e hora da detecção;

5.6.5.43.4.5. Mecanismo que gerou a detecção (varredura agendada, manual, em tempo real);

5.6.5.43.4.6. Nome da máquina/endereço IP;

5.6.5.43.4.7. Ação realizada;

5.6.5.43.4.8. Usuário logado no sistema;

5.6.5.44. Deverá buscar por itens de atualização nos repositórios, configurado pela gerência, de acordo com topologia e políticas especificadas;

5.6.5.45. Deverá possibilitar mais de uma versão da ferramenta e seus insumos, para que em casos de incompatibilidades decorrentes de atualizações, seja possível reinstalar versões anteriores estáveis ou instalar versões novas em grupos específicos, para fins de testes de compatibilidade antes de instalação em todo parque;

5.6.5.46. Deverá fornecer informações do status do agente e de seus componentes, através da gerência com informações atualizadas com delay máximo de 5 minutos;

5.6.5.47. Deve ser disponibilizado nos idiomas: português (preferencialmente) ou inglês;

5.6.6. Garantia e atualização das licenças, para servidores

5.6.6.1. A garantia técnica deverá ser contratada junto ao fabricante da solução, e sua vigência não poderá ser inferior ao período de 60 (sessenta) meses, contados a partir da aceitação definitiva da solução;

5.6.6.2. O atendimento do serviço de suporte técnico da garantia deverá ser feito por intermédio da CONTRATADA ou diretamente com a fabricante através de portal específico para fins de suporte ou por e-mail;

5.6.6.3. A garantia técnica deverá ser acionada nas situações específicas onde a CONTRATADA não conseguir solução para o problema ou quando o problema for detectado em relação aos elementos da solução contratada, tais como bugs ou algum mal funcionamento;

5.6.6.4. A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução;

5.6.6.5. As atualizações deverão ser fornecidas independente de solicitação da CONTRATANTE.

5.6.6.6. Deverão ser providas atualizações das listas de definições de vírus e demais insumos para funcionamento atualizado da solução, de acordo com o mercado;

5.6.6.7. Deverá permitir atualizações da engine do agente (software), assim como da base de dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução;

5.6.6.8. A garantia técnica contempla suporte técnico do fabricante, serviços de manutenções e atualizações da solução antivírus, base de dados de vacinas, bem como disponibilização de:

5.6.6.8.1. Solução de problemas que afetem elementos da solução, incluindo os softwares, atualizações e instalação, evoluções, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;

5.6.6.8.2. Manuais dos produtos e serviços ofertados, base de conhecimento para soluções conhecidas, canal de comunicação, esclarecimento de dúvidas e quaisquer outras informações solicitadas pela CONTRATANTE:

5.6.6.8.2.1. As informações prestadas deverão ser disponibilizadas preferencialmente no idioma Português do Brasil ou na falta deste, obrigatoriamente no idioma em Inglês;

5.6.6.8.3. Novas versões da solução lançadas pelo fabricante e lançamento de novos softwares em substituição da solução contratada, em caso de descontinuação do software fornecido.

5.6.6.9. Os serviços descritos neste item deverão ser prestados mediante abertura de chamado pela CONTRATANTE ou pela CONTRATADA, diretamente no portal de comunicação e suporte do fabricante, realizado por meio de e-mail e site de helpdesk;

5.6.6.10. A garantia deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia.

5.7. SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO

5.7.1. O serviço de suporte técnico especializado deverá ser prestado pela CONTRATADA durante o prazo de 12 (doze) meses, contados a partir da aceitação definitiva da solução.

5.7.2. O atendimento do serviço de suporte técnico, incluindo telefone, e-mail, presencial ou outros que se fizerem necessários, deverá ser realizado no idioma Português do Brasil;

5.7.3. O serviço de suporte deverá incluir a operacionalização das atualizações do fabricante para a solução, assim como serviços de manutenções da solução antivírus, base de dados de vacinas, com garantia completa dos serviços prestados:

5.7.3.1. O serviço técnico deverá contemplar a solução de problemas que afetem elementos da solução, atualizações, problemas de instalação, evoluções, patches, aplicação e implantação de correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;

5.7.4. Os serviços descritos neste item deverão ser prestados mediante abertura de chamado pela CONTRATANTE, realizado por meio de contato telefônico 0800, e-mail e site de helpdesk, quando houver, e em regime 24x7:

5.7.4.1. Para cada serviço técnico prestado a CONTRATADA deverá fornecer um identificador para a chamada realizada, acompanhando o nome do responsável pelo tratamento do chamado;

5.7.4.2. Toda e qualquer ação realizada pela CONTRATADA no ambiente da CONTRATANTE só poderá ser realizada com anuência e autorização da CONTRATANTE e por meio de acompanhamento de representante indicado para tal fim;

5.7.5. A CONTRATADA deverá fornecer relatório mensal dos chamados efetuados ou de chamado específico, contendo a data e hora da abertura por chamado, data e hora de cada atendimento realizado, a descrição do problema abordado e das ações realizadas e data do fechamento do chamado, após aceite por parte da CONTRATANTE.

5.7.6. Os serviços de suporte técnico e manutenção deverão ser realizados na modalidade remota, conforme critérios estabelecidos:

5.7.7. Os chamados deverão ser classificados conforme a severidade, de acordo com as definições da tabela abaixo:

Categoria	Nível	Descrição
Urgente	1	Serviços totalmente indisponíveis. Falha em servidor de produção que deixe indisponível os recursos do mesmo (serviço parado). Impacto a múltiplos usuários e/ou falha em servidor de produção que afete operações críticas da JF-1.
Crítico	2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos. Falha intermitente em serviços suportados que torne o ambiente inoperante. Impacto individual ou a pequenos grupos. Operação normal afetada, mas sem interrupção.
Não Crítico	3	Serviços disponíveis com ocorrência de alarmes de avisos, consulta sobre problemas, dúvidas gerais sobre a ferramenta antivírus. Manutenção e monitoramento de eventos de falhas ou de avisos relatados pelo cliente. Pequeno impacto a um ou mais usuários. A correção pode ser feita de maneira agendada, em um momento futuro.

5.7.8. A CONTRATADA deverá atender os chamados com prazo de início e término de acordo com a tabela a seguir:

Modalidade	Prazos de Atendimento	Níveis de severidade		
		1-Urgente	2-Crítico	3-Não crítico
E-mail, remoto, ou telefone.	Início	2 horas	4 horas	8 horas
	Término	12 horas	24 horas	72 horas

5.7.9. Entende-se como término de atendimento a solução definitiva do incidente ou redução de sua criticidade, a partir do qual será considerado o prazo limite do novo nível de criticidade.

5.8. TREINAMENTO

5.8.1. Deverão ser abordados no treinamento, no mínimo, os seguintes assuntos:

5.8.1.1. Informações e conhecimento sobre arquitetura, funcionamento e componentes envolvidos na solução.

5.8.1.2. Conhecimento da usabilidade e operação da solução, envolvendo:

5.8.1.3. Instalação e configuração dos componentes da gerência.

5.8.1.4. Gerência de políticas, tarefas e demais atividades oferecidas pela gerência da solução (criação e configuração).

5.8.1.5. Instalação e configuração dos agentes.

5.8.1.6. Criação e execução de consultas e relatórios

5.8.2. O treinamento deve ser realizado de segunda a sexta-feira (dias úteis), entre 8h (oito) horas e 18h (dezoito) horas.

5.8.3. O treinamento deve ter carga horária mínima de 16 (dezesseis) horas, limitado a 4h/aula diárias.

5.8.4. O treinamento será realizado para no mínimo 5 (cinco) alunos e no máximo 10 (dez) alunos simultaneamente.

5.8.5. O treinamento deverá ser realizado por videoconferência.

5.8.6. A Contratada deverá fornecer aos participantes do treinamento os certificados de conclusão de curso contendo, no mínimo:

5.8.6.1. Nome da empresa que ministrou a capacitação;

5.8.6.2. Nome do curso;

5.8.6.3. Nome do servidor capacitado;

5.8.6.4. Data de início e término da capacitação;

5.8.6.5. Carga horária;

5.8.6.6. Conteúdo programático.

5.8.7. Os certificados deverão ser entregues no prazo de 10 (dez) dias corridos contados após o término do treinamento.

5.8.8. Ao final do treinamento, os servidores participantes efetuarão uma avaliação do conteúdo ministrado. A qualidade será medida de 1 (um) a 10 (dez) pontos em cada um dos seguintes critérios:

5.8.8.1. Pontualidade;

5.8.8.2. Didática do instrutor;

5.8.8.3. Eficiência no repasse do conteúdo;

5.8.8.4. Adequação do treinamento ao conteúdo exigido no item 5.8.1 deste Anexo;

5.8.8.5. Adequação da carga horária.

5.8.9. Caso a média das avaliações seja inferior a 7 (sete) pontos, o fornecedor deverá refazer o treinamento, após as adequações necessárias, especialmente de substituição do Instrutor, e sem qualquer custo adicional para a TRF1, sendo que esse novo treinamento também será submetido aos mesmos critérios de avaliação.

5.8.10. A realização de novo treinamento substitutivo deverá ocorrer em até 60 (sessenta) dias corridos, em data proposta pelo fornecedor e aprovada pela TRF1.

5.8.11. O fornecedor arcará com despesas de encargos tributários, bem como transporte e alimentação do instrutor.

6. AMBIENTE TECNOLÓGICO

6.1. Plataforma de Hardware e software

6.1.1. Sistemas operacionais utilizados em servidores:

6.1.1.1. Windows Server 2012 (64 bits) e superiores.

6.1.1.2. Linux Server (64 bits).

6.1.2. Software utilizados nas estações clientes:

6.1.2.1. Windows 8.1 e 10;

6.1.2.2. Antivírus McAfee.

6.1.3. Browsers de mercado:

6.1.3.1. Chrome;

6.1.3.2. Internet Explorer;

6.1.3.3. Mozilla Firefox;

6.1.3.4. Microsoft Edge.

6.1.4. Ambiente de virtualização:

6.1.4.1. VMware Vsphere;

6.1.4.2. Oracle Virtualization Machine;

6.1.4.3. Microsoft Hyper-V.

6.1.5. Ferramentas de backup:

6.1.5.1. NetBackup.

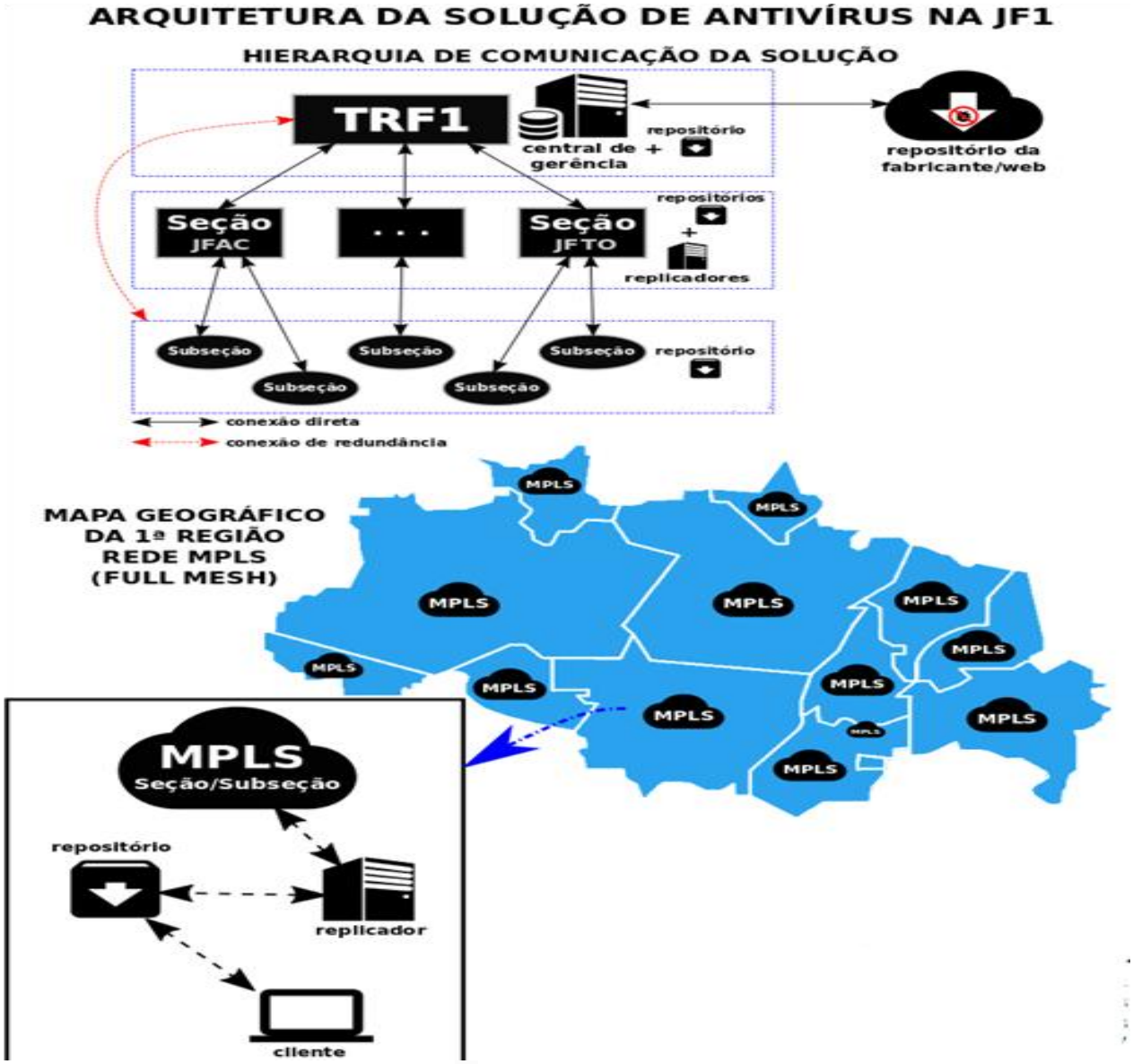
6.2. Informações gerais:

RESUMO ANALÍTICO DE ATIVOS DE INFRAESTRUTURA		
ID	**DESCRIÇÃO**	**QUANTIDADE ESTIMADA**
01	CPDs	67
02	Servidores Físicos (hosts)	300
03	Servidores Virtuais Linux	944
04	Servidores Virtuais Windows	614
05	Microcomputadores	12.784

6.3. Ciclo de Vida:

6.3.1. O TRF1 procura adotar ciclo de vida de 5 (cinco) anos para todos os ativos de Datacenter.

6.4. Figura 1 - do Mapa Arquitetural:



7. GARANTIA TÉCNICA, ATUALIZAÇÃO E SERVIÇOS DE INSTALAÇÃO E DESINSTALAÇÃO

7.1. Garantia técnica e atualização

7.1.1. A garantia técnica deverá ser contratada junto ao fabricante da solução, e sua vigência não poderá ser inferior ao período de 60 (sessenta) meses, contados a partir da aceitação definitiva da solução;

7.1.2. O atendimento do serviço de suporte técnico da garantia, deverá ser feito por intermédio da CONTRATADA ou diretamente com a fabricante através de portal específico para fins de suporte ou por e-mail;

7.1.3. A garantia técnica deverá ser acionada nas situações específicas onde a CONTRATADA não conseguir solução para o problema ou quando o problema for detectado em relação aos elementos da solução contratada, tais como bugs ou algum mal funcionamento;

7.1.4. A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução;

7.1.4.1. As atualizações de vacina deverão ser fornecidas independente de solicitação da CONTRATANTE.

7.1.4.2. Deverão ser providas atualizações das listas de definições de vírus e demais insumos para funcionamento atualizado da solução, de acordo com o mercado;

7.1.4.3. Deverá permitir atualizações da engine do agente (software), assim como da base de dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução;

7.1.5. A garantia técnica contempla suporte técnico do fabricante, serviços de manutenções e atualizações da solução antivírus, base de dados de vacinas, bem como disponibilização de:

7.1.5.1. Solução de problemas que afetem elementos da solução, incluindo os softwares, atualizações e instalação, evoluções, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas;

7.1.5.2. Manuais dos produtos e serviços ofertados, base de conhecimento para soluções conhecidas, canal de comunicação, esclarecimento de dúvidas e quaisquer outras informações solicitadas pela CONTRATANTE:

7.1.5.2.1. As informações prestadas deverão ser disponibilizadas preferencialmente no idioma Português do Brasil ou na falta deste, obrigatoriamente no idioma em Inglês;

7.1.5.3. Novas versões da solução lançadas pelo fabricante e lançamento de novos softwares em substituição da solução contratada, em caso de descontinuação do software fornecido.

7.1.6. Os serviços descritos neste item, exceto os serviços descritos no item 7.1.4.1 deste Anexo, deverão ser prestados mediante abertura de chamado pela CONTRATANTE ou pela CONTRATADA, diretamente no portal de comunicação e suporte do fabricante, realizado por meio de e-mail e site de helpdesk;

7.1.7. A garantia deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia.

7.2. Serviços de instalação e desinstalação

7.2.1. Serviço de Desinstalação

7.2.1.1. A desinstalação do parque atual existente na JF1 deverá ser efetuada pela CONTRATADA;

7.2.1.2. A CONTRATANTE deverá fornecer as credenciais necessárias para a execução da desinstalação, como usuário com privilégio.

7.2.1.3. A estratégia a ser adotada na execução da desinstalação será previamente acordada entre o CONTRATANTE e a CONTRATADA.

7.2.1.4. A desinstalação da ferramenta existente deverá ocorrer de forma silenciosa para o usuário, sem necessitar de reboot do equipamento e sem solicitar ações do usuário da estação/servidor;

7.2.1.4.1. Em casos específicos onde seja necessário reboot, deverá ser informado para a CONTRANTE para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar;

7.2.1.5. O equipamento onde for instalado a nova solução deverá estar LIMPA e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações em que mais de 1 solução além da vigente por este certame estejam instaladas no equipamento ao mesmo tempo;

7.2.1.6. Problemas na execução da desinstalação do agente deverão ser imediatamente comunicadas a CONTRATANTE;

7.2.2. Serviço de instalação e configuração

7.2.2.1. A instalação deverá ocorrer em todo o âmbito da JF1;

7.2.2.2. A instalação do agente deverá pressupor desinstalação da solução anterior;

7.2.2.3. A instalação do agente deverá ser imperceptível para o usuário, de forma a não aparecer pop-ups, mensagens, caixas de diálogos solicitando ação de usuário e nem janelas modais, de forma a interromper de qualquer forma o usuário;

7.2.2.4. Os serviços de instalação devem compreender a configuração da gerência centralizada em nuvem ou a configuração dos equipamentos servidores virtuais para os componentes da solução on-premise, incluindo

appliance virtual da gerência centralizada, banco de dados da solução e demais componentes a serem utilizados pela solução de gerência;

7.2.2.5. Deverá possibilitar a instalação dos componentes da solução de forma a refletir a estrutura hierárquica da JF1, observando a ordem: TRF1 > Seção Judiciária > Subseção Judiciária e o gráfico arquitetural Figura 1: Mapa Arquitetural;

7.2.2.6. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as Seções e Subseções;

7.2.2.7. Deve permitir que se instale os agentes individualmente por computador ou em lote, para vários computadores;

7.2.2.8. A interoperabilidade entre os componentes da solução deverá ser configurada por políticas na gerência e utilizando protocolos seguros;

7.2.2.9. Deverá permitir que se programe através de políticas o agendamento da distribuição dos itens atualizados na gerência centralizada para os repositórios;

7.2.2.10. Ao final do processo de instalação a CONTRATADA deverá fornecer os seguintes relatórios:

7.2.2.10.1. Relação de todos os computadores contendo antivírus instalado, com no mínimo as seguintes informações, agrupados por localidade – Subseção/Seção/TRF1;

7.2.2.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção/Seção/TRF1, contendo no mínimo:

7.2.2.10.2.1. Versão de cada módulo da solução instalado;

7.2.2.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

7.2.2.10.2.3. Versão de demais bibliotecas ou catálogos que compõem a solução instalado;

7.2.2.10.2.4. Os relatórios serão utilizados para avaliar conformidade da prestação do serviço de instalação;

7.2.2.10.2.5. Serão comparados com o quantitativo de máquinas ativas na JF1, utilizando a seguinte fórmula para apurar o índice de instalação:

7.2.2.10.2.5.1. IND – Índice de instalação;

7.2.2.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

7.2.2.10.2.5.3. QLA – Quantidade licenças adquiridas;

7.2.2.10.2.5.4. Será dado aceite da solução quando o resultado da instalação IND possua valor igual ou superior a 0.8 – IND >= 0.8.

ANEXO II - PREGÃO ELETRÔNICO SRP Nº 24/2022

MODELO DE PLANILHA PARA FORMULAÇÃO DE PREÇOS

GRUPO	ITEM	DESCRIÇÃO	UN.	QUANT. TOTAL	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
	01	**Solução de antivírus, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses**, demais características de acordo com as especificações constantes do Anexo I: **Versão:**	LICENÇA	**19.284**		
	02	**Solução de antivírus, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses**, demais características de acordo com as especificações constantes do Anexo I: **Versão:**	LICENÇA	**3.122**		
	03	**Suporte especializado**, demais características de acordo com as especificações constantes do Anexo I:	MESES	**36**		
	04	**Treinamento**, demais características de acordo com as especificações constantes do Anexo I:	ALUNOS	**26**		
VALOR TOTAL DO GRUPO						

Os Grupos 1 e 2 possuem a mesma solução com os mesmos quantitativos registrados pois tratam-se de tipo de licenciamento distintos que foram assim distribuídos para ampliação da concorrência, este Tribunal irá homologar somente o lote/grupo de menor preço, devendo após aceitação da melhor proposta, cancelar o grupo que restar com o maior valor.

OBSERVAÇÕES:

Prazo de entrega, na última versão do software, por meio de chaves de acesso ao site do fabricante, de ___ (_____) **dias úteis**, contados a partir do recebimento da Ordem de Fornecimento;

Prazo de execução dos serviços de desinstalação, instalação e configuração, de ___ (_____) **dias úteis**, contados a partir do recebimento da Ordem de Fornecimento;

Prazo de início do serviço de treinamento, de __ (_____) **dias úteis**, contados do recebimento da ordem de execução de serviço, bem como, o **prazo de execução dos serviços de treinamento,** de ___ (_____) **dias úteis**, contados a partir do seu início;

Prazo de garantia e atualização das licenças**,** de **__ (_____) meses,** contados a partir da data de assinatura do Termo de Recebimento Definitivo;

Declaro que a empresa de acordo com a condição da empresa**, não está sob pena de interdição de direitos previstos na Lei nº 9.605, de 12.02.98** (Lei de Crimes Ambientais);

Declaro que de acordo com a condição da empresa **a empresa não pratica registro de oportunidade** junto ao fabricante;

Prazo de validade da proposta, de **___ (_____) dias**, contado do dia útil imediatamente posterior ao indicado no item 02 deste Edital;

A licitante deverá ofertar e indicar a última versão de software disponível pelo fabricante, na data da licitação.

Outras Observações:

1 - Além das condições constantes do subitem 4.2 deste Edital, **deverão constar da proposta os seguintes dados do REPRESENTANTE LEGAL que assinará o Contrato**:

a) nome completo:
b) e-mail:
c) telefone:
d) celular:
e) domicílio:

ANEXO III - PREGÃO ELETRÔNICO SRP Nº 24/2022

MODELO DE FORMULÁRIO DE AVALIAÇÃO TÉCNICA

1 O formulário a partir do modelo constante do presente anexo é de preenchimento obrigatório, e deverá fazer parte integrante da proposta técnica de cada licitante.

2 As propostas que não atenderem à totalidade das características obrigatórias serão desclassificadas.

3 O formulário deverá ser preenchido sob a seguinte orientação:

a) **Coluna "Página do Manual/catálogo/etc" com indicação do requisito comprovado: constar nome do documento comprobatório (catálogo / folder / manual) com indicação da Página e citação do conteúdo comprobatório do requisito** que contenha a informação que comprove a característica solicitada. Quaisquer comprovações baseadas em URLs do fabricante, na internet, deverão ser materializadas em documento que deverá ser anexado no Portal de Compras do Governo Federal, mesmo que de forma parcial.

ITEM DO EDITAL E DA ESPECIFICAÇÃO TÉCNICA	DOCUMENTO COMPROBATÓRIO (CATÁLOGO / FOLDER / MANUAL) COM INDICAÇÃO DA PÁGINA E CITAÇÃO DO CONTEÚDO COMPROBATÓRIO DO REQUISITO
ITEM 1 -	
1.1....	
1.2.....	
...	
ITEM 2 -	
2.1.	
2.2.	
...	
ITEM 5 -	
5.1.	
5.2.	
....	
ITEM 6 -	
6.1.	
6.2.	
....	

ANEXO IV - PREGÃO ELETRÔNICO SRP Nº 24/2022

MINUTA DA ATA DE REGISTRO DE PREÇOS

A União, por intermédio do **TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO,** com sede na Praça dos Tribunais Superiores, Bloco "A" – Brasília/DF, inscrito no CNPJ/MF n. 03.658.507/0001-25, representado pelo_____, Dr._____, nos termos das Leis n. 8.666, de 21 de junho de 1993, e n. 10.520, de 17 de julho de 2002, e dos Decretos n. 10.024, de 20 de setembro de 2019, n. 7.892, de 23 de janeiro de 2013, e demais normas legais aplicáveis, obedecidas as disposições contidas no instrumento convocatório e em face da classificação da proposta apresentada no Pregão Eletrônico n._____/20__, RESOLVE registrar o preço ofertado pelo Fornecedor Beneficiário_____, estabelecido no _____, inscrito no CNPJ sob o n._____, representado pelo Sócio,_____, conforme abaixo:

ITEM	**QUANTIDADE ANUAL ESTIMADA**	**PREÇO UNITÁRIO**	**PREÇO TOTAL**
1			
Especificação:			
2			
Especificação:			

Este Registro de Preços terá validade de 12 (doze) meses, contados da data da sua assinatura pelas partes, instante a partir do qual o instrumento será considerado apto a produzir seus jurídicos efeitos. O extrato desta Ata será publicado em órgão oficial da Administração.

As especificações técnicas e demais exigências constantes do Decreto n. 7.892/13, no Processo Administrativo n._____ e Pregão Eletrônico n. _____ integram esta Ata de Registro de Preços, independentemente de transcrição.

A presente Ata, após lida e achada conforme, é assinada pelos representantes legais do Tribunal Regional Federal da Primeira Região e do Fornecedor Beneficiário.

TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO (Gerenciador)

RAZÃO SOCIAL DA EMPRESA
(Nome do Representante Legal)

ANEXO V - PREGÃO ELETRÔNICO SRP Nº 24/2022

MINUTA DO CONTRATO

TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

CONTRATO TRF1 MINUTA 16424171

CONTRATO N. ____/2022 PARA FORNECIMENTO, DESINSTALAÇÃO, INSTALAÇÃO E CONFIGURAÇÃO DE LICENCIAMENTO DE SOLUÇÃO DE ANTIVÍRUS, QUE ENTRE SI CELEBRAM A UNIÃO, POR INTERMÉDIO DO TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO, E A _____.

CONTRATANTE: UNIÃO/Tribunal Regional Federal da Primeira Região, com registro no CNPJ/MF n. 03.658.507/0001-25 e sede no SAU/Sul, Quadra 02, Bloco A, Praça dos Tribunais Superiores, Brasília, doravante denominado **CONTRATANTE**, neste ato representado, conforme atribuições delegadas pelo Ato Presi n. 163 de 07/05/1991, por seu diretor-geral da Secretaria, **CARLOS FREDERICO MAIA BEZERRA**, brasileiro, CPF n. 480.325.571-72, RG n. 1.015.832 - SSP/DF, residente e domiciliado nesta Capital.

CONTRATADA: _____, inscrita no CNPJ/MF _____, sediada na _____, CEP: _____, tel/ fax: _____, doravante denominada **CONTRATADA**, neste ato representada por _____, brasileiro, CPF _____, RG _____, residente e domiciliado em _____.

As partes acima qualificadas celebram o presente instrumento, com observação ao constante no **Processo Administrativo Eletrônico n. 0013621-23.2021.4.01.8000 – TRF1** e com fundamento n a **Lei 10.520/2002; Decreto 7.174/2010; Lei Complementar 123/2006; Decreto 10.024/2019; Decreto 8.538/2015; Decreto 7.892/2013; Lei 8.666/1993; Pregão Eletrônico n. ___/2022: Ata de Registro de Preços n. ____/2022;** demais disposições regulamentares e mediante as seguintes cláusulas e condições:

1. DO OBJETO

1.1. O presente instrumento tem por objeto o fornecimento, desinstalação, instalação e configuração de licenciamento de solução de antivírus, com garantia e atualização de versões, bem como serviços de suporte especializado e treinamento, para as estações de trabalho e equipamentos servidores do Contratante, de acordo com as especificações, condições e observações constantes neste contrato.

2. DA FINALIDADE

2.1. A finalidade desta contratação é prover o Contratante de solução com vistas a mitigar o risco de infestação das estações de trabalho e equipamentos servidores por ameaças virtuais, bem como manter o controle das estações de trabalho com antivírus atualizado.

3. DAS OBRIGAÇÕES DA CONTRATADA

3.1. Por este instrumento, a Contratada obriga-se a:

3.1.1. Responsabilizar-se por todos os encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, tributos de qualquer espécie que venham a ser devidos em decorrência da execução do objeto contratado, bem como custos relativos ao deslocamento e estada de seus profissionais, caso existam.

3.1.2. Responsabilizar-se pelos danos causados diretamente ao Contratante ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução deste contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento realizado pelo Contratante.

3.1.3. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais/distrital, em consequência de fato a ela imputável e relacionado com o objeto deste contrato.

3.1.4. Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais a que o Contratante for compelido a responder

em decorrência desta contratação.

3.1.4.1. Na hipótese de haver ação judicial envolvendo terceiros, cujo objeto refere-se aos serviços prestados e/ou produtos fornecidos ao Contratante, a Contratada deverá adotar as providências necessárias no sentido de excluir o Contratante da lide. Não obtendo êxito na exclusão, e, se houver condenação, deverá reembolsar ao Contratante, no prazo improrrogável de 10 (dez) dias úteis, a contar da data do efetivo pagamento, as importâncias que tenha sido obrigado a pagar.

3.1.5. Manter, durante toda a vigência do contrato e em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no instrumento convocatório para a contratação.

3.1.6. Manter seus profissionais, quando nas dependências do Contratante, em perfeitas condições de apresentação e asseio, submetendo-os às normas internas de conduta, segurança e disciplina e ao Código de Conduta da Justiça Federal, sem que se configure, com isso, qualquer vínculo empregatício com o órgão.

3.1.7. Substituir, no prazo estabelecido pelo Contratante, qualquer um de seus empregados que for considerado inconveniente à boa ordem, demonstre incapacidade técnica, perturbe a ação da fiscalização do Contratante, não acate as suas determinações ou não observe às normas internas do Contratante.

3.1.8. Prestar todos os esclarecimentos que forem solicitados pela fiscalização do Contratante, obrigando-se a atender todas as reclamações a respeito da execução do objeto contratado.

3.1.9. Comunicar ao Contratante, de imediato e por escrito, qualquer irregularidade verificada durante a execução do objeto deste contrato, para a adoção das medidas necessárias à sua regularização.

3.1.10. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todos os dados ou informações do Contratante ou suas representações obtidas em função da execução do objeto contratado, além de qualquer assunto de interesse do Contratante ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, devendo orientar seus profissionais nesse sentido.

3.1.10.1. Com a assinatura deste contrato, a Contratada compromete-se com os termos do seu Anexo I, denominado Compromisso de Confidencialidade de Informações, sobre as condições de revelação de informações sigilosas e as regras definidas para o seu uso e proteção.

3.1.11. Fornecer toda a documentação técnica original, completa e atualizada, contendo os manuais e guias de instalação, podendo ser em meio eletrônico.

3.1.12. Iniciar a prestação dos serviços de suporte técnico imediatamente após emissão do Termo de Recebimento Definitivo dos itens 01, 02, 05 e 06.

3.1.13. Implementar no ambiente do Contratante as evoluções tecnológicas necessárias para execução dos serviços contratados.

3.1.14. Garantir a qualidade do software em suas características operacionais, de manutenção, desempenho e consumo de hardware, durante o período de suporte.

3.1.15. Comunicar ao Contratante, por escrito, quando verificar condições inadequadas ou a iminência de fatos que possam prejudicar a perfeita prestação do serviço.

3.1.16. Utilizar as melhores práticas, capacidade técnica, materiais, softwares, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço, o atendimento às especificações contidas neste contrato e seus anexos.

3.1.16.1. A solução deve adequar-se às necessidades de negócio e técnicas estabelecidas pela segurança do Contratante. É necessário considerar a infraestrutura existente, bem como sua integração eficiente.

3.1.17. Participar, por intermédio do preposto ou, se for o caso, de representante específico credenciado a decidir em seu nome, de todas as reuniões e de atividades de coordenação, planejamento, acompanhamento e avaliação, que venham a ser convocadas pelo Contratante.

3.1.18. Cumprir a execução dos serviços e atualização de versões, sempre que necessário, em tempo, forma e regime de horário devidamente estabelecidos pelo Contratante.

3.1.19. Garantir ao Contratante que o conjunto de software licenciado para uso não infrinja quaisquer patentes, direitos autorais.

3.1.20. Promover, em no máximo 05 (cinco) dias úteis, as substituições das licenças em caso de falhas ou erros que impossibilitem as instalações dos conjuntos de software, respeitadas as condições normais de uso.

3.1.21. Assegurar ao Contratante, em caso de descontinuidade de qualquer produto da solução, e durante a vigência contratual, o direito ao uso de qualquer produto que o substitua.

3.1.22. Apresentar solução de contorno, nos casos em que foram detectados vírus novos cujas vacinas existentes não sejam eficazes, até a liberação de uma nova vacina específica para o caso.

3.1.23. Disponibilizar profissionais qualificados para realização do suporte técnico e curso de capacitação, conforme exigência contidas no Anexo II deste contrato.

3.1.24. Adaptar-se a mudanças, quando da evolução da arquitetura, sendo facultada a vistoria, sem que isso implique acréscimo nos preços contratados e sem quaisquer custos adicionais para o Contratante.

3.1.25. Apresentar no prazo de 10 (dez) dias após a emissão da ordem de fornecimento, o cronograma de execução da implantação da solução (desinstalação da solução em uso no Contratante e Seções e Subseções Judiciárias e instalação da nova solução), observados os prazos máximos de definidos neste contrato.

3.1.26. Responsabilizar, durante a prestação do suporte técnico on site, pelo custeio do deslocamento do profissional ao local da prestação de serviço, bem como por todas as despesas de transporte, diárias, hospedagem, seguro ou quaisquer outros custos envolvidos nos atendimentos das chamadas.

3.1.27. Prover os serviços de suporte técnico, incluindo o suporte do fabricante, tendo capacitação para analisar problemas de configuração e funcionamento, bem como parametrização, interoperabilidade e incompatibilidade do software, e a integração do mesmo com o ambiente do Contratante.

> 3.1.27.1. A identificação e a comunicação formal de defeito de software deverão ser feitas dentro do prazo de garantia, devendo a correção ser realizada ainda que a conclusão do serviço extrapole o prazo de garantia.

3.1.28. Informar ao Contratante o número do telefone para fins de esclarecimento de dúvidas relativas aos itens contratados, assim como para orientação e acompanhamento da solução de problemas quando não for demandada a presença de um técnico, a critério do Contratante.

3.1.29. Informar página na Internet, do fabricante do(s) software(s), onde estejam disponíveis as últimas versões do(s) software(s) e informações sobre correções e reporte de problemas, sem restrições de acesso público ou via cadastramento de pessoas autorizadas para o acesso. A página deverá conter, ainda, documentação técnica detalhada do(s) software(s) ofertado(s).

3.1.30. Possibilitar ao Contratante fazer quaisquer ajustes de configuração em quaisquer funcionalidades da solução contratada, para adequação ao ambiente onde está instalado, sem prejuízo dos serviços de suporte.

> 3.1.30.1. Caso o Contratante solicite, a Contratada deverá fornecer, durante todo o período da garantia, as orientações para que os ajustes sejam realizados, sem nenhum ônus adicional ao Contratante.
>
> 3.1.30.2. Caso seja necessário que se efetue algum downgrade na solução ou em algum item da solução para adequação ou contorno de algum problema detectado, o serviço deverá ser executado pela Contratada e sem ônus adicionais para a Contratante, até que seja disponibilizada algum “fix” que torne possível manter a solução do Contratante atualizada, de acordo com os padrões do fabricante.

4. DAS OBRIGAÇÕES DO CONTRATANTE

4.1. Por este instrumento, o Contratante obriga-se a:

4.1.1. Proporcionar todas as condições necessárias para que a Contratada possa cumprir o objeto deste contrato.

4.1.2. Emitir Ordem de Fornecimento das licenças (Desinstalação e instalação), nos termos do subitem 14.1 deste contrato.

4.1.3. Emitir Ordem de Execução dos Serviços (Treinamento).

4.1.4. Prestar informações e esclarecimentos que venham a ser solicitados pela Contratada, necessários à execução deste contrato.

4.1.5. Comunicar à Contratada qualquer irregularidade verificada na execução do contrato, determinando, de imediato, as providências necessárias à sua regularização.

4.1.6. Acompanhar e fiscalizar, rigorosamente, o cumprimento deste contrato.

4.1.7. Designar servidor ou comissão para acompanhar e fiscalizar o contrato.

4.1.8. Disponibilizar cópia da norma de segurança da informação e das demais normas pertinentes à execução dos serviços.

4.1.9. Convocar os representantes da Contratada para realização de reunião inicial, para alinhamento de expectativas contratuais.

4.1.10. Atestar o recebimento da solução e da prestação dos serviços fornecidos pela Contratada que estejam em conformidade com as especificações e prazos definidos neste contrato, conforme inspeções realizadas.

4.1.11. Recusar o recebimento do objeto que não estiver em conformidade com as especificações constantes da proposta apresentada pela Contratada.

4.1.12. Avaliar relatório e estatísticas dos serviços executados pela Contratada, observando as metas de níveis mínimos de serviço.

4.1.13. Emitir, explicitamente, decisão sobre todas as solicitações e reclamações relacionadas à entrega dos bens, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a entrega das soluções, no prazo máximo de 01 (um) mês, contado do recebimento pelo Contratante, podendo ser prorrogado, motivadamente, por igual período.

4.1.14. Vetar o emprego de qualquer produto ou serviço que considerar incompatível com as especificações estabelecidas e que possa ser inadequado, nocivo ou danificar seus bens patrimoniais ou ser prejudicial à saúde dos servidores ou de terceiros.

4.1.15. Permitir ao pessoal técnico da Contratada, desde que devidamente identificado, o acesso aos equipamentos de propriedade do Contratante para a execução dos serviços contratados, respeitadas as normas de segurança vigentes em suas dependências;

4.1.16. Comunicar à Contratada eventuais alterações de tecnologias citadas neste contrato ou em uso no Contratante.

4.1.17. Fornecer os acessos necessários para que a Contratada possa realizar a devida instalação/ desinstalação da solução adquirida.

4.1.18. Exigir, sempre que necessário, a apresentação da documentação pela Contratada que comprove a manutenção das condições que ensejaram a sua contratação.

5. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

5.1. O acompanhamento e a fiscalização do contrato consistem na verificação da conformidade da sua execução pelo gestor do contrato, de acordo com as cláusulas contratuais estabelecidas.

5.2. A gestão será exercida por servidor ou comissão designada pelo Contratante.

5.3. O gestor do contrato de que trata o subitem 5.2 desta cláusula deverá ainda:

5.3.1. Anotar em registro próprio todas as ocorrências relacionadas com a execução do objeto contratado, determinando à Contratada o que for necessário à regularização das faltas ou defeitos

observados.

5.3.2. Promover todas as ações necessárias para a regularização das faltas ou defeitos observados no cumprimento deste contrato.

5.3.3. Comunicar formalmente à Contratada as irregularidades cometidas.

5.3.4. Autorizar, receber e atestar os documentos da despesa, quando comprovado a fiel e correta execução dos serviços, para fins de pagamento.

5.3.5. Propor as glosas na(s) Nota(s) Fiscal (is)/Fatura(s) em decorrência de objeto não executado.

5.3.6. Controlar o prazo de vigência do instrumento contratual sob sua responsabilidade.

5.3.7. Acompanhar a execução desta contratação de forma a alcançar o cumprimento integral da execução do seu objeto.

5.3.8. Encaminhar às autoridades competentes eventuais pedidos de alteração e prorrogação contratual, observando os requisitos legais e contratuais.

5.3.9. Manter registro de aditivos.

5.3.10. Comunicar à autoridade superior, em tempo hábil e por escrito, as situações que impliquem atraso e descumprimento de cláusulas contratuais, para adoção dos procedimentos necessários à aplicação das sanções contratuais cabíveis.

5.4. As decisões e providências que ultrapassarem a competência do gestor deverão ser solicitadas ao seu superior hierárquico em tempo hábil para a adoção das medidas convenientes.

5.5. Expirada a vigência do contrato, o gestor informará à autoridade competente acerca do integral cumprimento do objeto para fins de registros e respectivo controle financeiro-orçamentário.

5.5.1. Observado o disposto no subitem 13.1.2 e não havendo pendências quanto a sua execução, o servidor ou comissão oficiará à Contratada, se for o caso, acerca da devolução da garantia prestada na forma do art. 56, § 1º, da lei 8666/1993.

6. DO LOCAL E PRAZO DE ENTREGA E EXECUÇÃO DOS SERVIÇOS

6.1. As licenças deverão ser disponibilizadas, na última versão do software, por meio de chave de acesso no site do fabricante a ser enviada via e-mail para: TRF1 - sesei@trf1.jus.br; SJMG - nutec.mg@trf1.jus.br; e UFT - nati@uft.edu.br, no prazo máximo de **10 (dez) dias úteis** contados do recebimento da Ordem de Fornecimento.

6.1.1. Deverão ser entregues juntamente com as chaves de acesso a documentação técnica e os manuais pertinentes aos softwares adquiridos.

6.1.2. A validação das licenças entregues será por meio de visualização na console de gerenciamento da solução, que deverá estar disponível para o cliente.

6.1.3. Entende-se por entrega da solução, objetos dos itens 01, 02, 05 e 06, a desinstalação e instalação e configuração das licenças.

6.1.4. Deverão ser iniciados os prazos de garantia e atualização das licenças após o aceite definitivo.

6.2. Os serviços de desinstalação, instalação e configuração deverão ser executados no prazo máximo de **44 (quarenta e quatro) dias úteis**, contados do recebimento provisório dos itens 01, 02, 05 e 06.

6.3. O serviço de suporte deverá ser iniciado após assinatura do termo de recebimento definitivo dos Itens 01, 02, 05 e 06.

6.4. O serviço de treinamento deverá ser iniciado no prazo máximo de **10 (dez) dias úteis**, contados do recebimento da ordem de execução de serviço.

6.4.1. O serviço de treinamento deverá ser finalizado com o prazo máximo de até **10 (dez) dias úteis**, contatos a partir do seu início.

6.5. Para execução dos serviços de instalação e suporte técnico a Contratada deverá entrar em contato com a equipe de fiscalização do contrato ou via e-mail para: TRF1 - sesei@trf1.jus.br; SJMG - nutec.mg@trf1.jus.br; e UFT - nati@uft.edu.br para que o Contratante disponibilize os meios de acesso

remoto ao ambiente tecnológico.

6.6. O treinamento deverá ser prestados de forma remota, devendo a Contratada enviar via e-mail para: TRF1 - sesei@trf1.jus.br; SJMG - nutec.mg@trf1.jus.br; e UFT - nati@uft.edu.br o link de acesso.

7. DA GARANTIA TÉCNICA, ATUALIZAÇÃO E SERVIÇOS DE INSTALAÇÃO E DESINSTALAÇÃO

7.1. Garantia técnica e atualização:

7.1.1. A garantia técnica deverá ser contratada junto ao fabricante da solução, e sua vigência não poderá ser inferior ao período de 60 (sessenta) meses, contados a partir da aceitação definitiva da solução.

7.1.2. O atendimento do serviço de suporte técnico da garantia deverá ser feito por intermédio da Contratada ou diretamente com o fabricante através de portal específico para fins de suporte ou por e-mail.

7.1.3. A garantia técnica deverá ser acionada nas situações específicas onde a Contratada não conseguir solução para o problema ou quando o problema for detectado em relação aos elementos da solução contratada, tais como bugs ou algum mal funcionamento.

7.1.4. A garantia técnica deverá incluir o fornecimento das atualizações do fabricante para a solução.

7.1.4.1. As atualizações de vacina deverão ser fornecidas independente de solicitação do Contratante.

7.1.4.2. Deverão ser providas atualizações das listas de definições de vírus e demais insumos para funcionamento atualizado da solução, de acordo com o mercado.

7.1.4.3. Deverá permitir atualizações da engine do agente (software), assim como da base de dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução.

7.1.5. A garantia técnica contempla suporte técnico do fabricante, serviços de manutenções e atualizações da solução antivírus, base de dados de vacinas, bem como disponibilização de:

7.1.5.1. Solução de problemas que afetem elementos da solução, incluindo os softwares, atualizações e instalação, evoluções, patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos, adequações e esclarecimento de dúvidas.

7.1.5.2. Manuais dos produtos e serviços ofertados, base de conhecimento para soluções conhecidas, canal de comunicação, esclarecimento de dúvidas e quaisquer outras informações solicitadas pelo Contratante:

7.1.5.2.1. As informações prestadas deverão ser disponibilizadas preferencialmente no idioma Português do Brasil ou na falta deste, obrigatoriamente no idioma em Inglês.

7.1.5.3. Novas versões da solução lançadas pelo fabricante e lançamento de novos softwares em substituição da solução contratada, em caso de descontinuação do software fornecido.

7.1.6. Os serviços descritos neste subitem 7.1, exceto os serviços descritos no subitem 7.1.4.1, deverão ser prestados mediante abertura de chamado pelo Contratante ou pela Contratada, diretamente no portal de comunicação e suporte do fabricante, realizado por meio de e-mail e site de helpdesk.

7.1.7. A garantia deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia.

7.2. Serviços de instalação e desinstalação:

7.2.1. Serviço de Desinstalação:

7.2.1.1. A desinstalação do parque atual existente no Contratante deverá ser efetuada pela Contratada.

7.2.1.2. O Contratante deverá fornecer as credenciais necessárias para a execução da desinstalação, como usuário com privilégio.

7.2.1.3. A estratégia a ser adotada na execução da desinstalação será previamente acordada entre o Contratante e a Contratada.

7.2.1.4. A desinstalação da ferramenta existente deverá ocorrer de forma silenciosa para o usuário, sem necessitar de reboot do equipamento e sem solicitar ações do usuário da estação/servidor.

7.2.1.4.1. Em casos específicos onde seja necessário reboot, deverá ser informado para o Contratante para que se monte uma estratégia de forma a não interromper o fluxo de trabalho onde se necessitar.

7.2.1.5. O equipamento onde for instalado a nova solução deverá estar LIMPO e sem vestígios da instalação anterior, de forma que não se acarrete crashes e erros na instalação do novo agente e que não ocorra situações em que mais de 01 (uma) solução além da vigente por este contrato estejam instaladas no equipamento ao mesmo tempo.

7.2.1.6. Problemas na execução da desinstalação do agente deverão ser imediatamente comunicadas o Contratante.

7.2.2. Serviço de instalação e configuração:

7.2.2.1. A instalação deverá ocorrer em todo o âmbito do Contratante.

7.2.2.2. A instalação do agente deverá pressupor desinstalação da solução anterior.

7.2.2.3. A instalação do agente deverá ser imperceptível para o usuário, de forma a não aparecer pop-ups, mensagens, caixas de diálogos solicitando ação de usuário e nem janelas modais, de forma a interromper de qualquer forma o usuário.

7.2.2.4. Os serviços de instalação devem compreender a configuração da gerência centralizada em nuvem ou a configuração dos equipamentos servidores virtuais para os componentes da solução on-premise, incluindo appliance virtual da gerência centralizada, banco de dados da solução e demais componentes a serem utilizados pela solução de gerência.

7.2.2.5. Deverá possibilitar a instalação dos componentes da solução de forma a refletir a estrutura hierárquica do Contratante, observando a ordem: TRF1 > Seção Judiciária > Subseção Judiciária e o gráfico arquitetural Figura 1: Mapa Arquitetural.

7.2.2.6. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as Seções e Subseções.

7.2.2.7. Deve permitir que se instale os agentes individualmente por computador ou em lote, para vários computadores.

7.2.2.8. A interoperabilidade entre os componentes da solução deverá ser configurada por políticas na gerência e utilizando protocolos seguros.

7.2.2.9. Deverá permitir que se programe através de políticas o agendamento da distribuição dos itens atualizados na gerência centralizada para os repositórios.

7.2.2.10. Ao final do processo de instalação a Contratada deverá fornecer os seguintes relatórios:

7.2.2.10.1. Relação de todos os computadores contendo antivírus instalado, com no mínimo as seguintes informações, agrupados por localidade – Subseção/Seção/TRF1.

7.2.2.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção/Seção/TRF1, contendo no mínimo:

7.2.2.10.2.1. Versão de cada módulo da solução instalado.

7.2.2.10.2.2. Versão da DAT ou catálogo de vacinas instalado.

7.2.2.10.2.3. Versão de demais bibliotecas ou catálogos que compõem a solução instalado.

7.2.2.10.2.4. Os relatórios serão utilizados para avaliar conformidade da prestação do serviço de instalação.

7.2.2.10.2.5. Serão comparados com o quantitativo de máquinas ativas no Contratante, utilizando a seguinte fórmula para apurar o índice de instalação:

a. IND – Índice de instalação.

b. QAI – Quantidade de computadores com antivírus instalado.

c. QLA – Quantidade licenças adquiridas.

d. Será dado aceite da solução quando o resultado da instalação IND possua valor igual ou superior a 0.8 – IND >= 0.8.

8. DO RECEBIMENTO

8.1. O objeto deste contrato será recebido da seguinte forma:

8.1.1. Para os itens 01 e 02 do objeto o recebimento se dará da seguinte forma:

8.1.1.1. Provisoriamente, no prazo máximo de 10 (dez) dias úteis, após a entrega das licenças, por Ordem de Fornecimento, mediante Termo de Recebimento Provisório.

8.1.1.1.1. O recebimento provisório consiste na identificação e conferência da solução entregue e o **licenciamento devidamente aplicado na console de gerenciamento**, observada a necessidade de conclusão da implantação da gerencia centralizada e de no mínimo 10% do quantitativo da ordem de fornecimento distribuídas em pelo menos 3 localidades da 1ª região, com ênfase na avaliação dos quantitativos e verificação da adequação da marca, versão e itens de maior relevância do produto fornecido em comparação com Proposta Comercial.

8.1.1.1.2. Caso seja identificado problema ou pendência na solução, o Contratante notificará a Contratada e o prazo para o recebimento provisório estabelecido no subitem 8.1.1.1 ficará suspenso a contar da data do envio da notificação até a data de resolução do problema ou pendência, sem prejuízo à aplicação das glosas e sanções contratualmente previstas.

8.1.1.2. Definitivamente, no prazo máximo de 10 (dez) dias úteis, contados do término da instalação e configuração da solução em todo o ambiente do Contratante, mediante Termo de Recebimento Definitivo assinado pelas partes.

8.1.1.2.1. O recebimento definitivo consiste na verificação do atendimento aos requisitos técnicos da solução e sua integral operabilidade no ambiente do Contratante.

8.1.1.2.2. Caso seja identificado problema ou pendência na solução, o Contratante notificará a Contratada e o prazo para o recebimento definitivo estabelecido no subitem 8.1.1.2 ficará suspenso a contar da data do envio da notificação até a data de resolução do problema ou pendência, sem prejuízo à aplicação das glosas e sanções contratualmente previstas.

8.1.1.3. A solução poderá ser recusada nos seguintes casos:

8.1.1.3.1. Quando entregue com especificações técnicas inferiores ou divergentes das contidas neste contrato.

8.1.1.3.2. Quando identificado avarias ou defeitos.

8.1.2. Para o item 03 do objeto o recebimento se dará da seguinte forma:

8.1.2.1. Definitivamente, no prazo máximo de 15 (quinze) dias corridos, contados a partir do 1º dia útil subsequente ao recebimento do documento de cobrança.

8.1.2.2. A Contratada deverá encaminhar, mensalmente, até no 1ª dia útil do mês subsequente ao da prestação dos serviços, documento de cobrança para análise do gestor do contrato e aplicação dos níveis mínimos de serviço.

8.1.2.3. Os serviços poderão ser recusados no todo ou em parte nos seguintes casos:

8.1.2.3.1. Quando não foram atingidos os níveis mínimos de serviço ou quando não forem atendidos os requisitos estabelecidos neste contrato e em seus anexos.

8.1.2.3.2. Quando identificados defeitos ou outras inconformidades.

8.1.3. Para o item 04 do objeto o recebimento se dará da seguinte forma:

8.1.3.1. Provisoriamente, no prazo máximo de 15 (quinze) dias corridos após o encerramento da Ordem de Execução dos Serviços, mediante Termo de Recebimento Provisório.

8.1.3.2. Definitivamente, no prazo máximo de 15 (quinze) dias corridos, contados a partir da data de assinatura do Termo de Recebimento Provisório.

8.1.3.3. Os serviços poderão ser recusados no todo ou em parte nos seguintes casos:

8.1.3.3.1. Quando não foram atingidos os níveis mínimos de serviço ou quando não forem atendidos os requisitos estabelecidos neste contrato e em seus anexos.

8.1.3.3.2. Quando identificados defeitos ou outras inconformidades.

8.2. Níveis Mínimos de Serviço Exigidos e Glosas aplicáveis:

8.2.1. Os Indicadores e glosas serão aferidos nos termos abaixo descritos:

IAE – INDICADOR DE ATRASO	
Tópico	Descrição
Finalidade	Medir o tempo de atraso na entrega dos produtos e/ou na conclusão dos serviços.
Meta a cumprir	IAE < = 0 | A meta definida visa garantir a entrega dos produtos e serviços dentro do prazo previsto.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio do Contratante e a serem acompanhadas pela Contratada.
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrado na Ordem de Fornecimento, na Ordem de Execução de Serviços ou nos prazos definidos no contrato, incluindo os prazos de atendimento dos chamados. Será subtraída a data de conclusão (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data prevista para o início da execução do serviço ou da contagem do prazo de entrega. Será subtraída a hora da conclusão do atendimento (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela hora de abertura do chamado, para os prazos computados em horas.
Periodicidade	De acordo com a demanda.
Mecanismo de Cálculo (métrica)	IAE = TEX – TESTOnde:IAE – Indicador de Atraso de Entrega; TEX – Tempo de Execução – corresponde ao período de execução, da sua data de início até a data de término. A data ou hora de início será aquela constante na OES/OF ou da abertura do chamado; caso não esteja explícita, será o primeiro dia útil após a emissão ou abertura.A data ou hora de entrega ou conclusão deverá ser aquela reconhecida pelo fiscal técnico. Para os casos em que o fiscal técnico rejeita a entrega/conclusão, o prazo de execução continua a correr, findando-se apenas quando houver aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução – constante na OES/OF ou no contrato.
Observações	Obs1: Serão utilizados dias e horas úteis na medição. Obs2: Os dias com expediente parcial na JF1 serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador quando a execução for cancelada por solicitação da Contratante.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: 0 dias ou 0 horas – Pagamento integral; Glosa de 1%, por dia ou hora de atraso, sobre o valor da parcela em atraso ou sobre o valor mensal dos serviços, até o limite de 20%. A partir do 21º dia ou hora, para os prazos em hora, deverá ser aplicada, cumulativamente as penalidades contratualmente previstas.
ID – INDICADOR DE DEFEITO	
Tópico	Descrição
Finalidade	Medir a quantitativo de defeitos nos serviços e produtos entregues pela Contratada. Considera defeito quando o serviço ou produto não atende a necessidade, ou não resolve o problema, ou não atende ao requisito de qualidade mínimo exigido.

Meta a cumprir	ID = 0
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio do Contratante e a serem acompanhadas pela Contratada.
Forma de acompanhamento	Quantidade de defeitos identificados nos produtos e serviços entregues referentes à Ordem de Execução de Serviços ou chamados atendidos pelo fornecedor, sem justificativa aceita pelo TRF1.
Periodicidade	Mensalmente
Mecanismo de Cálculo (métrica)	ID = Total de defeitos por OES (quando se tratar de atendimento por OES) ID = Total de chamados recusados ou total de chamados cujo o problema não foi solucionado *Somar o total de defeitos apurados após o encerramento da OES ou total de defeitos apurados no mês.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **ID**: ≤ 2 – Pagamento integral De 3 até 5 – Glosa de 2,5% sobre da fatura mensal ou valor da OES. De 6 até 8 – Glosa de 5,0% sobre da fatura mensal ou valor da OES. De 9 até 11 – Glosa de 7,5 % sobre da fatura mensal ou valor da OES. De 12 ou mais - Glosa de 10% sobre o faturamento mensal ou valor da OES.
OBSERVAÇÃO: Os referidos indicadores são cumulativos, portanto podem ser aplicados simultaneamente, ficando a glosa total limitada ao percentual máximo de 20% do bem ou serviço a que se referir a avaliação.	

9. DA DOTAÇÃO ORÇAMENTÁRIA

9.1. A despesa com a execução do presente contrato correrá à conta dos recursos orçamentários consignados no Programa de Trabalho _____ e Elemento de Despesa __.__.__.

9.2. Foi emitida a Nota de Empenho _____, em _____, no valor de R$ _____ (_____), para atender as despesas oriundas desta contratação.

10. DO PREÇO

10.1. O Contratante pagará à Contratada, pelo objeto deste contrato, os valores estabelecidos no Anexo IV deste contrato.

10.2. O preço constante desta cláusula compreende todas as despesas concernentes ao objeto deste contrato, bem como todos os impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, seguro e outras despesas de qualquer natureza que se façam indispensáveis à perfeita execução do objeto desta contratação, já deduzidos os abatimentos eventualmente concedidos.

11. DO REAJUSTE

11.1. Os preços deste contrato, **referente ao item 03 (Suporte técnico especializado)**, poderão ser reajustados, desde que observado o interregno mínimo de um ano, a contar da data limite para apresentação da proposta, constante do instrumento convocatório.

11.1.1. São nulos de pleno direito quaisquer apuração de índice de reajuste que produza efeito financeiro equivalente aos de reajuste de periodicidade inferior à anual.

11.2. O reajuste dos preços terá como limite a variação do ICTI – Índice de Custo de Tecnologia da Informação - ou, na hipótese de extinção deste, por outro que venha a substituí-lo.

11.3. Caberá à Contratada solicitar o reajustamento dos preços e demonstrar a variação, mediante apresentação da respectiva planilha, bem como apresentar a documentação comprobatória do seu pleito.

11.4. No caso de eventual prorrogação contratual, nos reajustamentos subsequentes ao primeiro, o valor do contrato será reajustado após o interregno de um ano, que será contado a partir da data do fato gerador que deu ensejo ao último reajuste.

11.4.1. As alterações decorrentes de reajustamentos serão formalizadas mediante Termo de Apostilamento.

11.5. Para fins de concessão do reajuste poderão ser realizadas diligências visando conferir a variação de custos alegada pela Contratada, considerando-se:

11.5.1. Os preços praticados no mercado e em outros contratos da Administração Pública.

11.5.2. As particularidades deste contrato.

11.5.3. Indicadores setoriais, valores oficiais de referência, tarifas públicas ou outros equivalentes; e

11.5.4. A disponibilidade orçamentária do Contratante.

11.6. O prazo para a Contratada solicitar o reajuste encerra-se na data da prorrogação/término de vigência contratual, obedecendo ao seguinte:

11.6.1. Caso a Contratada não solicite o reajuste tempestivamente, dentro do prazo acima fixado, ocorrerá a preclusão do direito ao reajuste.

11.6.2. Nessas condições, se a vigência do contrato tiver sido prorrogada, novo reajuste só poderá ser pleiteado após o decurso de novo interregno mínimo de 1 (um) ano, contado da prorrogação contratual.

11.6.3. Se até a data da prorrogação contratual, ainda não tiver sido solicitado/concedido o reajuste, caberá a Contratada solicitar a reserva de seu direito para ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão, com vistas à inclusão de cláusula no termo aditivo de prorrogação para resguardar o direito futuro ao reajuste, nos termos do subitem 14.1.2.5 deste contrato.

11.7. Os novos valores contratuais reajustados produzirão efeitos:

11.7.1. A partir da ocorrência do fato gerador que deu causa ao reajuste.

11.7.2. Em data futura, desde que acordada entre as partes, sem prejuízo da contagem de periodicidade para concessão dos próximos reajustes.

11.8. Os reajustamentos não interferem no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com fundamento no art. 65, II, “d”, da Lei nº 8.666, de 1993.

12. DO PAGAMENTO

12.1. O pagamento será efetuado em **até 15 (quinze) dias úteis**, contados do atesto do documento de cobrança.

12.2. O atesto de que trata o subitem anterior será realizado da seguinte forma:

12.2.1. Para os itens 01 e 02 do objeto:

12.2.1.1. 1ª atesto - 30% (trinta por cento) após o recebimento provisório, por ordem de fornecimento.

12.2.1.2. 2ª atesto - 70% (setenta por cento) após o recebimento definitivo.

12.2.2. Para o item 03 do objeto, os serviços serão atestados mensalmente, no prazo estabelecido no subitem 8.1.2.1 deste contrato.

12.2.3. Para o item 04 do objeto, os serviços serão atestados por ordem de execução de serviço, no prazo estabelecido no subitem 8.1.3.2 deste contrato.

12.3. A regularidade de que trata o subitem 3.1.5, especialmente com o Fundo de Garantia do Tempo de Serviço – FGTS (Certificado de Regularidade de Situação do FGTS – CRF) e a Receita Federal e Dívida Ativa da União (Certidão Conjunta de Débitos relativos à Tributos Federais e à Dívida Ativa da União), será confirmada antes do pagamento

12.4. Havendo atraso no prazo estipulado no subitem 12.1 desta Cláusula, não ocasionado por culpa da Contratada, o valor devido será corrigido monetariamente, pelo Índice de Preços ao Consumidor Amplo - IPCA, relativo ao período compreendido entre a data do vencimento do prazo para pagamento e a da sua efetivação.

12.4.1. A Contratada deverá formular o pedido, por escrito, ao Contratante, acompanhado da respectiva memória de cálculo e do respectivo documento de cobrança.

12.5. Os pagamentos serão creditados em nome da Contratada, mediante ordem bancária em conta corrente por ela indicada ou por meio de ordem bancária para pagamento de faturas com código de barras, desde que satisfeitas às condições estabelecidas neste contrato.

12.6. Os pagamentos, mediante a emissão de qualquer modalidade de ordem bancária, serão realizados desde que a Contratada efetue a cobrança de forma a permitir o cumprimento das exigências legais, principalmente no que se refere às retenções tributárias.

12.7. Havendo erro no documento de cobrança, ausência da documentação necessária ao pagamento, ou outra circunstância que desaprove a liquidação da despesa, o prazo para o pagamento será interrompido até que a Contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte do Contratante.

12.8. O pagamento será retido ou glosado, sem prejuízo das sanções cabíveis, quando:

12.8.1. A Contratada não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas.

12.8.2. A Contratada deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

12.8.3. Se por qualquer motivo alheio à vontade do Contratante for paralisada a prestação dos serviços, sendo que o período correspondente não gerará obrigação de pagamento.

12.9. O Contratante poderá deduzir do montante a pagar os valores correspondentes a eventuais multas, inclusive aquelas em processo de apuração, ou indenizações, devidas pela Contratada, nos termos deste contrato.

12.10. Os pagamentos estarão sujeitos à retenção na fonte dos tributos, conforme legislação vigente.

13. DA GARANTIA DO CONTRATO

13.1. Objetivando assegurar o fiel cumprimento deste contrato, a Contratada deverá apresentar a garantia contratual, numa das modalidades previstas no § 1.º do art. 56 da Lei 8.666/1993, no prazo de 10 (dez) dias úteis contados da data inicial estabelecida no subitem 14.1 deste contrato.

13.1.1. A Garantia será no valor de **R$ _____ (_____)**, correspondente a 5% (cinco por cento) do valor total contratado.

13.1.2. O prazo da garantia deverá abranger o período de execução do contrato e se estender por até 3 (três) meses após o termo final da vigência do contrato, com vencimento previsto para _____.

13.1.3. No caso de apresentação de garantia na modalidade caução em dinheiro, a Contratada deverá efetuar o depósito na Caixa Econômica Federal, Agência 2301 – PAB – Tribunal Regional Federal da 1ª Região.

13.2. É obrigação de a Contratada fazer constar do documento de garantia, expressamente, sua vinculação a esta cláusula contratual.

13.3. A garantia deverá ser renovada/endossada a cada prorrogação ou alteração, reajustes/repactuações do contrato, no prazo de 10 (dez) úteis, contados da assinatura do termo aditivo ou da notificação, na hipótese de reajustes/repactuações realizados mediante apostila ao contrato.

13.4. A garantia, independente da modalidade escolhida, deverá assegurar:

13.4.1. Pagamento imediato pela ocorrência de quaisquer eventos danosos previstos no contrato, notadamente os relativos a multas moratórias e/ou compensatórias, mediante simples apresentação, pelo Contratante, do valor apurado ou fixado de acordo com as pertinentes cláusulas deste contrato.

13.4.2. Cobertura de prejuízos causados ao Contratante, decorrentes de culpa ou dolo da Contratada na execução do contrato, apurados em regular processo administrativo, até o limite previsto no subitem 13.1.1

13.4.3. Renúncia expressa aos benefícios do art. 827 do Código Civil Brasileiro, na hipótese de apresentação de garantia na modalidade de fiança bancária. (Lei nº 10.406/2002).

13.5. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à Contratada.

13.6. No caso de penalidade imposta pelo Contratante, basta a apresentação da decisão final exarada no processo administrativo para que o correspondente valor seja recolhido ao erário, no prazo máximo de 30 (trinta) dias, na forma fixada pelo Contratante, independentemente de anuência, autorização ou

manifestação da Contratada.

13.7. Sancionada a Contratada, caso esta não realize o pagamento no prazo fixado, correspondente valor será exigido do garantidor mediante simples comunicação escrita.

13.8. Se o valor da garantia ou parte desta for utilizado para pagamento dos eventos indicados nos subitens 13.4.1 e 13.4.2 desta cláusula, obriga-se a Contratada a efetuar a respectiva reposição ou complementação, no prazo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação feita pelo Contratante.

13.9. Em caso de alteração do contrato, a Contratada deverá apresentar nova garantia na mesma modalidade da anterior ou complementar a já existente, no prazo previsto no subitem anterior.

13.10. Caso a Contratada não cumpra o disposto nos itens anteriores, dentro do prazo estipulado, o Contratante poderá reter cautelarmente o valor da garantia dos pagamentos devidos, até a apresentação da garantia, sendo todo o ônus decorrente de responsabilidade da Contratada.

13.10.1. Em caso de retenção de que trata o subitem 13.10, o Contratante oficiará a Contratada para, em novo prazo de até 5 (cinco) dias úteis contados da data da notificação, regularizar a prestação da garantia.

13.11. A garantia, ou seu saldo, será liberada ou restituída conforme o disposto no subitem 5.5 deste contrato, desde que cumpridas todas as obrigações contratuais.

14. DA VIGÊNCIA

14.1. Este contrato entra em vigor a partir de _____ e sua vigência compreenderá os seguintes prazos:

14.1.1. Para os itens 01 e 02:

14.1.1.1. Até 10 (dez) dias úteis para a emissão e entrega da Ordem de Fornecimento, contados da data inicial estabelecida no subitem 14.1 deste contrato, com término previsto para _____.

14.1.1.2. Até 10 (dez) dias úteis para a disponibilização da solução, contados a partir do recebimento da Ordem de Fornecimento, com término previsto para _____.

14.1.1.3. Até 44 (quarenta e quatro) dias úteis para o término dos serviços de desinstalação, instalação e configuração, contados a partir do recebimento provisório, com término previsto para _____.

14.1.1.4. Até 10 (dez) dias úteis para emissão do Termo de Recebimento Provisório da solução, contados da entrega das licenças, com término previsto para _____.

14.1.1.5. Até 10 (dez) dias úteis, para emissão do Termo de Recebimento Definitivo da solução, contados do término da instalação e configuração da solução em todo o ambiente do Contratante, com término previsto para _____.

14.1.1.6. Até 60 (sessenta) meses de vigência da garantia técnica, contados a partir do recebimento definitivo da solução, com término previsto para _____.

14.1.2. Para o item 03:

14.1.2.1. Vigorará por **12 (doze) meses**, contados do recebimento definitivo de que trata o subitem 14.1.1.5, podendo ser prorrogado por igual período ou fração, mediante acordo entre as partes, por meio de termo aditivo, até o limite de 60 (sessenta) meses, incluindo os primeiros 12 (doze) meses.

14.1.2.2. Este instrumento, relativo ao item 03, tem seu término previsto para _____.

14.1.2.3. O último dia de vigência do contrato corresponderá à transição contratual para fins de prorrogação ou nova contratação, e não repercutirá como execução financeira, conforme o Anexo V deste contrato.

14.1.2.4. Para o encaminhamento do pedido de prorrogação do contrato, o gestor do contrato deve observar os seguintes requisitos:

14.1.2.4.1. Prestação regular dos serviços.

14.1.2.4.2. Manutenção do interesse do Contratante na realização do serviço.

14.1.2.4.3. Permanência da vantagem econômica para o Contratante.

14.1.2.4.4. Manifestação expressa da Contratada quanto ao interesse na prorrogação.

14.1.2.4.5. Verificação se houve declaração de inidoneidade ou suspensão da Contratada no âmbito da União ou do Contratante.

14.1.2.5. Caso, na data da prorrogação contratual, ainda não tenha sido possível proceder aos cálculos devidos para fins de reajuste do contrato, caberá à Contratada no ato que manifestar anuência com a prorrogação, requerer a inclusão de cláusula no termo aditivo de prorrogação garantindo o seu direito ao reajuste, sob pena de preclusão, conforme previsão contida no subitem 11.6.3 deste contrato.

14.1.2.6. O Contrato não será prorrogado quando a Contratada tiver sido declarada inidônea ou suspensa no âmbito da União ou do Contratante, enquanto perdurarem os efeitos.

15. DAS SANÇÕES ADMINISTRATIVAS

15.1. Em caso de descumprimento das obrigações previstas neste instrumento, poderão ser aplicadas as seguintes sanções:

a) Advertência.

b) Multa.

c) Impedimento de licitar e contratar com a União pelo prazo de até cinco anos (art. 7º da Lei 10.520/2002, c/c o art. 49 do Decreto 10.024/2019).

15.1.1. As sanções previstas nas alíneas "a" e "c" do subitem 15.1 desta cláusula poderão ser aplicadas juntamente com a da alínea "b" do mesmo subitem.

15.2. A penalidade fundada em comportamento ou conduta inidônea ensejará impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos, na forma do disposto no art. 49 do Decreto 10.024/2019.

15.3. O atraso injustificado na entrega/execução do objeto desta contratação ou qualquer outro inadimplemento contratual, com exceção dos previstos nos subitens 8.2.1, 15.4 e 15.7 desta cláusula, sujeitará a contratada à multa de 0,5% (cinco décimos por cento) por dia de atraso, calculada sobre o valor do item em atraso, até o limite de 10 (dez) dias.

15.3.1. A partir do 11º dia, a multa por dia será de 1% (um por cento), até o limite de 8% (oito por cento), considerado o limite total de 13% (treze por cento) da multa cumulada com a penalidade do subitem 15.3.

15.4. O descumprimento dos prazos de atendimento dos chamados por parte da Contratada, por período superior ao previsto no subitem 8.2.1 deste contrato, ensejará a aplicação da multa de 1% (um por cento) sobre o valor unitário do objeto, por dia de atraso, até o limite de 04 (quatro) dias corridos.

15.4.1. A partir do 5º dia, a multa diária passa a ser de 2% (dois por cento), até o limite de 10% (dez por cento), considerado o limite total de 14% (quatorze por cento) da multa cumulada com a penalidade do subitem 15.4.

15.5. Nas hipóteses em que não haja prefixação do termo inicial ou final para cumprimento de obrigações, o Contratante, mediante hábil notificação, fixará os prazos a serem cumpridos. O descumprimento da obrigação no prazo fixado constituirá em mora a Contratada, hipótese que incidirá a sanção prevista no subitem 15.3.

15.6. A inexecução parcial ou total deste instrumento, por parte da Contratada, poderá ensejar a resolução contratual, com cancelamento do saldo de empenho e a aplicação da multa no percentual de 15% (quinze por cento) sobre a parte não entregue/executada ou sobre o valor total contratado, respectivamente.

15.7. Se em decorrência de ação ou omissão, que não resulte em inexecução parcial ou total do objeto contratado, o cumprimento da obrigação se tornar inútil em momento posterior e não tiver sido objeto de multa anterior, a Contratada estará sujeita à multa de 0,5% (cinco décimos por cento) sobre o valor total do contrato e por ocorrência.

15.7.1. O valor da multa de que trata o subitem 15.7 não poderá ser superior àquela que seria cabível

caso a obrigação tivesse sido entregue em mora.

15.8. A Contratada, quando não puder cumprir os prazos estipulados para o cumprimento das obrigações decorrentes desta contratação, deverá apresentar justificativa por escrito, devidamente comprovada, acompanhada de pedido de prorrogação, nos casos de ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições deste contrato; ou que impeça a sua execução, por fato ou ato de terceiro reconhecido pela Administração em documento contemporâneo à sua ocorrência.

15.8.1. A solicitação de prorrogação, contendo o novo prazo para execução, deverá ser encaminhada ao Contratante até o vencimento do prazo inicialmente estipulado, ficando exclusivamente a critério do Contratante a sua aceitação.

15.8.2. O pedido de prorrogação extemporâneo ou não justificado na forma disposta nesta cláusula será prontamente indeferido, sujeitando-se a Contratada às sanções previstas neste instrumento.

15.9. Descumprida a obrigação no prazo fixado, poderá o Contratante, por exclusiva vontade, estabelecer data-limite para seu cumprimento, hipótese que não elidirá a multa moratória prevista no subitem 15.3.

15.10. A inobservância do prazo fixado para apresentação da garantia contratual acarretará a aplicação de multa de 0,5% (cinco décimos por cento) sobre o valor da garantia não prestada, por dia de atraso, observado o máximo de 10% (dez por cento).

15.10.1. O atraso superior a 25 (vinte e cinco) dias na apresentação da garantia autoriza o Contratante a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, com as cominações legais cabíveis.

15.11. Na hipótese de descumprimento de obrigações pós-contratuais, a Contratada arcará com os custos de tantas quantas forem necessárias novas contratações para suprir respectivas falhas, sem prejuízo das sanções previstas neste instrumento.

15.11.1. A exclusivo critério do Contratante, as perdas e os danos poderão ser exigidos mediante simples levantamento do prejuízo.

15.11.2. O ressarcimento do prejuízo referido nos subitens 15.11 e 15.11.1 será obtido por meio da garantia contratual prestada e, se insuficiente, será cobrado da ora Contratada, ainda que judicialmente.

15.12. O valor das multas poderá ser deduzido dos créditos existentes em favor da Contratada, descontado da garantia contratual ou recolhido ao Tesouro Nacional, no prazo de 5 (cinco) dias úteis, contados a partir da data da notificação, ou, ainda, quando for o caso, cobrados judicialmente (art. 86 da Lei 8.666/1993).

15.13. A aplicação de quaisquer das penalidades previstas neste instrumento será precedida de regular processo administrativo, assegurados o contraditório e a ampla defesa.

15.14. O Contratante promoverá o registro no SICAF de toda e qualquer penalidade imposta à Contratada.

16. DA RESCISÃO

16.1. O Contratante se reserva o direito de rescindir unilateralmente o presente contrato, na ocorrência de qualquer das situações previstas no art. 78, incisos I a XII e XVII e art. 79, inciso I, todos da Lei 8.666/1993.

16.2. O presente Contrato poderá, ainda, ser rescindido por acordo entre as partes ou judicialmente, nos termos constantes no art. 79, incisos II e III, da Lei 8.666/1993.

17. DA PUBLICAÇÃO

17.1. O presente Contrato será publicado em forma de extrato, no D.O.U, em conformidade com o disposto no parágrafo único do art. 61 da Lei 8.666/1993.

18. DAS DISPOSIÇÕES FINAIS

18.1. Toda e qualquer comunicação/informação/notificação/intimação e envio de documentos (contrato e demais documentos) à Contratada será feita pelo e-mail informado no preâmbulo deste contrato, ou outro que o substitua, apontado formalmente pela Contratada.

18.2. É de exclusiva responsabilidade da Contratada o fornecimento e manutenção de e-mail atualizado,

até mesmo na hipótese de obrigações pós-contratuais.

18.3. Em caso de inobservância do previsto no subitem 18.2, o Contratante poderá realizar a comunicação/informação/notificação/intimação via postal/pessoal.

18.4. Frustradas as tentativas na forma do subitem 18.3, o Contratante poderá realizar a comunicação/informação/notificação/intimação da Contratada mediante publicação no Diário da Justiça Federal da 1ª Região – e-DJF1, disponível no site do Contratante (http://portal.trf1.jus.br/portaltrf1/publicacoes/diarios-da-justica/diarios-da-justica.htm), para todos os efeitos, ressalvadas as hipóteses legais em que se determine publicação no Diário Oficial da União.

19. DO FORO

19.1. Fica eleito pelas partes o foro federal, no Distrito Federal, para dirimir quaisquer dúvidas decorrentes do presente contrato, com renúncia de qualquer outro.

E por estarem justas e contratadas, as partes assinam o presente instrumento por meio de senha eletrônica.

CARLOS FREDERICO MAIA BEZERRA
Diretor-Geral da Secretaria do TRF 1ª Região

CONTRATADA

Documento assinado eletronicamente por **Webes Ribeiro da Silva**, **Supervisor(a) de Seção**, em 29/08/2022, às 14:58 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf1.jus.br/autenticidade informando o código verificador **16424171** e o código CRC **C8BFA6AD**.

ANEXO I AO CONTRATO N. _____/2022
COMPROMISSO DE CONFIDENCIALIDADE DE INFORMAÇÕES

1. OBJETO

1.1. Este compromisso estabelece condições específicas para regulamentar as obrigações a serem observadas pela Contratada, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo Contratante, por força dos procedimentos necessários para a execução deste contrato, de acordo com o que dispõem a Lei 12.527/2011 e os Decretos 7.724/2012 e 7.845/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo, bem como o que dispõe a Lei 13.709/2018 e a Resolução CNJ 363/2021 sobre a proteção geral de dados.

2. CONCEITOS E DEFINIÇÕES

2.1. Para os efeitos deste compromisso, são estabelecidos os seguintes conceitos e definições:

2.1.1. INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

2.1.2. INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

2.1.3. CONTRATO: contrato celebrado entre as partes, ao qual este ANEXO se vincula.

3. INFORMAÇÃO SIGILOSA

3.1. Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado.

3.2. Este compromisso abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de

computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do Contratante e/ou quaisquer informações técnicas / comerciais relacionadas / resultantes ou não ao Contrato, doravante denominadas INFORMAÇÕES, a que diretamente ou pelos seus empregados a Contratada venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do Contrato.

4. LIMITES DO SIGILO

4.1. As obrigações constantes deste ANEXO não serão aplicadas às INFORMAÇÕES que:

4.1.1. Sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da Contratada.

4.1.2. Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente ANEXO.

4.1.3. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5. DIREITOS E OBRIGAÇÕES

5.1. A Contratada se compromete a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do contrato, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do contrato.

5.2. A Contratada se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do Contratante.

5.3. A Contratada compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do contrato sobre a existência deste ANEXO, bem como da natureza sigilosa das informações.

5.3.1. A Contratada deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente ANEXOe dará ciência ao Contratante dos documentos comprobatórios.

5.4. A Contratada obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do Contratante, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo Contratante.

5.5. Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste ANEXO.

5.5.1. Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

5.6. A Contratada obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à Contratada, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do contrato.

5.7. A Contratada, na forma disposta no subitem 5.2 acima, também se obriga a:

5.7.1. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas.

5.7.2. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas

derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros.

5.7.3. Comunicar ao Contratante, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente.

5.7.4. Identificar as pessoas que, em nome da Contratada, terão acesso às informações sigilosas.

5.8. A contratada deverá comunicar ao Contratante, em até 02 (dois) dias úteis, contadas do instante do conhecimento, a ocorrência de acessos não autorizados a dados pessoais, de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou de qualquer outra forma de tratamento inadequado, suspeito ou ilícito, sem prejuízo das medidas previstas no art. 48 da Lei 13.709/2018 (LGPD).

6. DURAÇÃO DO SIGILO

6.1. O presente COMPROMISSO tem natureza irrevogável e irretratável, e seus efeitos terão vigência desde a assinatura do contrato até expirar o prazo de classificação da informação a que a Contratada teve acesso em razão da execução do objeto contratado ou àquele determinado em lei.

7. PENALIDADES

7.1. A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão deste contrato. Neste caso, a Contratada estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo Contratante, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme art. 87 da Lei 8.666/1993.

8. DISPOSIÇÕES GERAIS

8.1. Este compromisso de confidencialidade é parte integrante e inseparável do contrato.

8.2. Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

8.3. O disposto no presente ANEXO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

8.4. Ao assinar o contrato, a Contratada manifesta sua concordância no sentido de que:

8.4.1. O Contratante terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da Contratada.

8.4.2. A Contratada deverá disponibilizar, sempre que solicitadas formalmente pelo Contratante, todas as informações requeridas pertinentes ao contrato.

8.4.3. A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo.

8.4.4. Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes.

8.4.5. O presente compromisso somente poderá ser alterado mediante termo aditivo firmado pelas partes.

8.4.6. Alterações do número, natureza e quantidade das informações disponibilizadas para a Contratada não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste ANEXO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento.

8.4.7. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das

informações disponibilizadas para a Contratada, serão incorporados a este ANEXO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas.

8.5. Este COMPROMISSO não deve ser interpretado como criação ou envolvimento das partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

ANEXO II AO CONTRATO N. ____/2022
ESPECIFICAÇÕES TÉCNICAS
Item 5 do Anexo I ao Edital

ANEXO III AO CONTRATO N. ____/2022
AMBIENTE TECNOLÓGICO
Item 6 do Anexo I ao Edital

ANEXO IV AO CONTRATO N. ____/2022
PLANILHA DE PREÇOS
(Conforme modelo do anexo II do Edital)

ANEXO V AO CONTRATO N. ____/2022
CRONOGRAMA DE DESEMBOLSO RELATIVO AO ITEM 03

Contrato:	_____/2022					
Empresa:						
Início				Término		
Mês	**Ano**					
	2022	**2023**	**2024**	**2025**	**2026**	**2027**
Janeiro						
Fevereiro						
Março						
Abril						
Maio						
Junho						
Julho						
Agosto						
Setembro						
Outubro						
Novembro						
Dezembro						
Total			**-**		**-**	
Valor Global do Contrato						