TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

TERMO DE REFERÊNCIA

INTRODUÇÃO	
Referência Normativa	Resolução 182 de 2013 do Conselho Nacional de Justiça e do Modelo de Contratações de Tecnologia da Informação da Justiça Federal - MCTI-JF.
Responsabilidade	Equipe de Planejamento da Contratação

1 - 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, de acordo com as especificações, condições e observações constantes neste Termo e em seus anexo.

2 - FINALIDADE

2.1. O presente termo tem por finalidade prover solução de antivírus para atender toda JF1 considerando que, nos termos da manifestação (13172836) constante do PAe (0023331-72.2018.4.01.8000), a empresa atualmente contratada não tem interesse na prorrogação do item 2 do contrato (serviço de suporte), único item passível de prorrogação conforme previsão contida na cláusula 16 do instrumento. Razão pela qual o Contrato 66/2018 (7294613) não será prorrogado.

3 - JUSTIFICATIVA

3.1. Motivação:

3.1.1. 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.

3.1.2. 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

3.1.3. 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.

3.1.4. 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).

3.1.5. 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.

3.1.6. 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*.

3.1.7. 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.

3.1.8. 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.

3.1.9. 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.

3.1.10. 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.

3.1.11. 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.

3.1.12. 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.

3.1.13. 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.

3.2. Benefícios Diretos e Indiretos:

3.2.1. Mitigar o risco de infestação das estações de trabalho e equipamentos servidores por ameaças virtuais.

3.2.2. Manter o controle das estações de trabalho com antivírus atualizado.

3.2.3. Aumentar a taxa de satisfação dos clientes internos e externos da JF1 com os serviços de TI.

3.2.4. Melhoria de nivelamento nos portes de tecnologia, capacitação e automação da 1ª Região.

3.2.5. Atualização tecnológica, proporcionando maior eficiência em relação aos trabalhos essenciais no âmbito da 1ª Região.

3.2.6. Maior rapidez na detecção de vírus e de ameaças virtuais.

3.2.7. Gestão de processos simplificada, já que, a partir de uma mesma tela, é possível proteger todos os computadores, dispositivos móveis e servidores de uma só vez.

3.2.8. Avisos e atualizações automáticas dos programas usados no JF1.

3.2.9. Controle de sites suspeitos, para evitar que sejam acessados e infectem o sistema da empresa.

3.2.10. Restrição do uso de dispositivos móveis (como, por exemplo, pendrives), que podem ser usados nas máquinas e infectar diversas estações de trabalho e equipamentos servidores ao mesmo tempo.

3.2.11. Auxílio de suporte técnico, incluindo suporte on-site em eventuais problemas ou dúvidas que possam aparecer durante o uso do software.

3.2.12. Reestabelecimento da proteção das estações de trabalhos e equipamentos servidores, proporcionando maior segurança para a execução dos trabalhos essenciais no âmbito da 1ª Região.

3.3. Correlação com o planejamento existente:

3.3.1. Contrato 66/2018 - 0023331-72.2018.4.01.8000 - com vigência até **27/09/2021**.

3.4. Referência a estudos preliminares que embasem a contratação:

3.4.1. A contratação pretendida vai ao encontro dos objetivos estratégicos do Tribunal. A presente contratação encontra-se em consonância com o planejamento existente, e as diretrizes dos macrodesafios do Poder Judiciário, no aperfeiçoamento da gestão de custos e melhoria da qualidade dos gastos públicos.

3.4.2. Cabe destacar, ainda, que este Termo de Referência foi elaborado seguindo o Decreto nº 7174/2010, a Resolução 182/2013 do CNJ e a Resolução 279/2013 do CJF. A Secretaria de Tecnologia da Informação-SECIN, realiza as suas aquisições de equipamentos, materiais e serviços de Tecnologia da Informação (TI) com base em seu PDTI e demais planos, conforme item 4.1 do Alinhamento Estratégico. Os artefatos que embasam a contratação foram elaborados em conformidade com o MCTI-JF, quais sejam: a) Estudo Técnico Preliminar (16142023), Mapa de Riscos (16142067) e o presente Termo de Referência.

4 - ALINHAMENTO ESTRATÉGICO E CLASSIFICAÇÃO ORÇAMENTÁRIA

4.1. A ação, objeto deste termo, está alinhada com os seguintes planos:

4.1.1. Plano Estratégico de Tecnologia da Informação da Justiça Federal – PETI para 2021/2026, aprovado pela resolução CJF-RES 685/2020.

4.1.1.1. id. 4. Promover e fortalecer a segurança da informação digital na Justiça Federal

4.1.2. Plano Diretor de Tecnologia da Informação da Justiça Federal da Primeira Região – PDTI-TRF1 2021/2023, aprovado pelo CGTI-JF1, PAe 0009898-93.2021.4.01.8000:

4.1.2.1. PDTI-INIC-65 - Manter atualizada a solução de antivírus da JF1.

4.1.3. Plano de Contratações de Tecnologia da Informação da Justiça Federal da Primeira Região – PCSTI-TRF1 2021, aprovado pelo CGTI-JF1, conforme consta na ata de reunião 12111010, PAe 0004687-23.2014.4.01.8000.

4.1.3.1. ID - Novas Contratações - Solução de segurança de estações de trabalho e servidores (antivírus).

4.2. Classificação Orçamentária:

4.2.1. Fonte: MTGI/AI

4.2.2. Valor: **R$ 5.262.516,32**

5 - BASE LEGAL

5.1. Modalidade de Licitação

5.1.1. Esta licitação será efetuada nos moldes do pregão eletrônico, conforme disposto na Lei 10.520/2002, regulamentada pelo Decreto 10.024/2019, visto se tratar de contratação de serviço comum, cujos padrões de desempenho e qualidade podem ser objetivamente definidos no edital, por meio de especificações usuais de mercado.

5.2. Adjudicação

5.2.1. Recomenda-se que o objeto seja adjudicado pelo **MENOR PREÇO POR GRUPO**, pois no presente caso a contratação de todos os itens em um único grupo se justifica em razão da necessidade de padronização, possível ganho de escala e interdependência existente entre os itens. Isso pois, a solução contratada deve ser a mesma para toda JF1 visando possibilitar que a solução de gerenciamento seja compatível com o licenciamento ofertado, considerando que o gerenciamento centralizado é um dos requisitos de negócio no presente caso.

5.2.2. Além disso o fornecedor responsável pela entrega, instalação e configuração das licenças deverá ser o mesmo a prestar o suporte técnico especializado, considerando que o fornecimento desse serviço acessório por empresa diversa da que fará a entrega e instalação das licenças poderá colocar em risco a qualidade e a disponibilidade da solução no ambiente tecnológico da JF1, sendo impraticável delimitar responsabilidades e ações, se houver mais de um fornecedor dentro do processo que envolve o fornecimento do bem e a execução dos serviços assessórios, além disso, é necessário que as licenças para estação de trabalho e servidores sejam fornecidas pelo mesmo fornecedor para não comprometer a eficácia da administração do parque tecnológico, principalmente em relação a rastreabilidade de eventos de segurança, para casos onde houver encadeamento de eventos envolvendo servidores e estações de trabalho, a ser fornecido pela funcionalidade de EDR, também justifica-se pela diminuição do tempo de resposta em caso de necessidade da intervenção manual da equipe. Ademais, também, justifica-se o não parcelamento do objeto no presente caso pelo aumento da eficiência administrativa por meio da otimização do gerenciamento do contrato.

5.2.3. Deste modo, o não parcelamento do objeto no presente caso não é uma afronta à Súmula 247 do TCU, conforme jurisprudências observadas nos Acórdãos 5.260/2011 – TCU – 1ª Câmara e 861/2013 – TCU – Plenário, que tratam de questões de economicidade e necessidade de padronização.

5.3. Do Registro de Preços

5.3.1. Deverá ser adotado o Sistema de Registro de Preços, uma vez que a presente contratação se amolda à previsão contida no inciso IV do Art. 3º do Decreto 7.892, de 23 de janeiro de 2013, pelos seguintes aspectos:

5.3.1.1. Pela conveniência do objeto vir a atender a mais de um órgão da Justiça Federal da Primeira Região e de não haver previsão imediata de aquisição para o objeto a ser registrado, considerando que os pedidos ocorrerão mediante demanda de cada unidade requisitante. Considerando que será avaliada qual solução ficará mais econômica, não foi possível definir previamente a solução a ser demandada. Não há previsão imediata de aquisição para as quantidades registradas, considerando que os pedidos ocorrerão sob demanda da unidade requisitante. Destaca-se que, após a realização do Pregão Eletrônico, será adquirida a solução/grupo que restar mais econômica para a administração.

5.3.1.2. Nos termos do Decreto 7.892/2013, será divulgada a IRP no intuito de possibilitar aos órgãos da Justiça Federal da Primeira Região se unirem para proceder apenas um certame licitatório do mesmo objeto;

5.3.1.3. No ato da homologação o sistema convocará as licitantes remanescentes, que poderão reduzir seus preços ao valor da proposta da licitante mais bem classificada, para formação do cadastro reserva.

5.3.1.4. 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 7892/2013).

5.3.1.5. A figuração do licitante no cadastro de reserva não obriga a administração à contratação.

5.3.1.6. Cancelado o registro de preço em relação ao vencedor da licitação (§1º do art. 11 do Decreto 7.892/2013), os demais licitantes que constem do cadastro de reserva poderão ser convocados, na mesma ordem de classificação da fase competitiva, para prosseguir na execução do serviço. Aceita a convocação e cumpridos os requisitos legais e regulamentares, nova Ata de Registro de Preços será editada em favor do novo beneficiário, permanecendo na condição de cadastro de reserva os licitantes integrantes da Ata original que permanecerão na ordem de classificação antes estabelecida.

5.3.1.7. Não serão admitidas adesões à Ata de Registro de Preços por órgãos não participantes, conforme determinação da SECAD 7147403, em razão da inexistência de norma complementar para regular o procedimento.

5.4. Do Órgão Gerenciador e Órgãos Participantes

5.4.1. O Órgão Gerenciador será o Tribunal Regional Federal da 1ª Região, com sede em Brasília - DF.

5.4.2. Dos Órgãos Participantes:

	ÓRGÃO	UASG
1	SEÇÃO JUDICIÁRIA DE MINAS GERAIS/MG	090013
2	FUNDAÇÃO UNIVERSIDADE FEDERAL DO TOCANTINS - UFT	154419

5.5. Do Direito de Preferência

5.5.1. Será assegurada preferência na contratação, nos termos do disposto no art. 3º da Lei nº 8.248, de 1991, regulado pelo art. 5º, do Decreto nº 7.174/2010, para fornecedores de bens e serviços, observada a seguinte ordem:

5.5.1.1. 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;

5.5.1.2. Bens e serviços com tecnologia desenvolvida no País;

5.5.1.3. Bens e serviços produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

6 - DESCRIÇÃO DO SERVIÇO

6.1. Serviços que compõem o objeto:

GRUPO	ITEM	DESCRIÇÃO DOS BENS E SERVIÇOS	UNIDADE DE MEDIDA	QTDS ESTIMADAS			BR SIASG CATMAT/CATSER	SUSTENTÁVEL (SIM/NÃO)
				POR ÓRGÃO		TOTAL		
1	1	Solução de antivírus com licenciamento perpétuo, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1	12.784	19.284	27472	Não se aplica
				SJMG	3.500			
				UFT	3.000			
		Solução de antivírus com licenciamento perpétuo, para equipamentos		TRF1	2.472			
				SJMG	450			

	2	servidores, com garantia e atualização da solução, pelo período de 60 meses	Licença	UFT	200	3.122	27464	Não se aplica
	3	Serviço de suporte técnico especializado	Meses	TRF1 SJMG UFT	12 12 12	36	22993	Não se aplica
	4	Treinamento	Alunos	TRF1 SJMG UFT	10 6 10	26	3840	Não se aplica
2	5	Solução de antivírus com licenciamento por meio de subscrição, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1 SJMG UFT	12.784 3.500 3.000	19.284	27502	Não se aplica
	6	Solução de antivírus com licenciamento por meio de subscrição, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1 SJMG UFT	2.472 450 200	3.122	27502	Não se aplica
	7	Serviço de suporte técnico especializado	Meses	TRF1 SJMG UFT	12 12 12	36	22993	Não se aplica
	8	Treinamento	Alunos	TRF1 SJMG UFT	10 6 10	26	3840	Não se aplica

6.1.1. Em caso de discordância existente entre as especificações descritas no Comprasnet (código BR) e as especificações técnicas constantes deste instrumento, prevalecerão as últimas.

6.1.2. 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.

6.1.3. ITEM 1,2, 5 e 6 - A quantidade de licenças a serem registradas foi estimada conforme detalhamento constante no item 3 do Estudo Técnico Preliminar (16142023).

6.1.4. ITEM 3 e 7- O suporte especializado deverá ser contratado na forma mensal.

6.1.5. ITEM 4 e 8 - Em relação ao treinamento a estimativa leva em consideração 6 servidores da Sesei e ao menos 1 servidor de cada área técnica envolvida na operação da solução Sesol e Sesof, bem como 2 servidores da Diatu.

6.1.6. Garantia e atualização, devem ser fornecidas exclusivamente pelo fabricante, pois trata-se das atualizações dos componentes da solução e fornecimento dos manuais oficiais, perdurando pela vigência do contrato, que não poderá ser inferior a 60 (sessenta) meses, a contar da data do recebimento definitivo da solução.

6.1.7. O suporte especializado tem a finalidade a solução de problemas que afetem elementos da solução, problemas de instalação, evoluções, patches, aplicação, adequações e esclarecimento de dúvidas no ambiente do TRF1.

6.1.8. O Grupo 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 proposta cancelar o grupo que ficou com o maior valor.

7 - PROPOSTA DAS LICITANTES

7.1. A proposta deverá ser identificada com a razão social e encaminhada, preferencialmente, em papel timbrado do licitante, contendo os seguintes itens:

7.1.1. As propostas devem descrever individualmente e com clareza a identificação da solução ofertada, as quantidades, os valores e outras informações aplicáveis.

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

7.1.3. Deverá, ainda, apresentar os seguintes documentos:

7.1.3.1. Declaração que ateste a não aplicação da prática de registro de oportunidade junto ao fabricante, conforme subitem 9.2.4.1.1 do Acórdão 2569/2018-TCU-Plenário.

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

7.3. Para os softwares, correspondentes aos itens de 01, 02, 05 e 06 do objeto, a contratada deve fazer acompanhar às propostas, preferencialmente por meio eletrônico, manuais, catálogos, folhetos, impressos, publicações originais do fabricante ou outros documentos suficientes para comprovação dos requisitos técnicos do software ofertado(tais como cópia de tela), bem como o formulário de avaliação técnica, conforme Anexo IV deste Termo, no qual deverá constar a identificação e página do documento comprobatório e o texto onde se encontra descrita cada uma das funcionalidades e características da solução ofertada.

7.3.1 Caso a licitante não disponha de catálogos, folhetos, impressos ou publicações originais do fabricante quanto às especificações técnicas, deverá apresentar declaração do fabricante da solução em questão com as referidas especificações.

8 - HABILITAÇÃO

8.1. Qualificação econômico-financeira:

8.1.1. A qualificação Econômico-Financeira será comprovada mediante a apresentação da seguinte documentação:

8.1.1.1. Certidão negativa de feitos sobre falência, expedida pelo distribuidor da sede da licitante.

8.1.1.2. 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).

8.1.1.3. 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 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.

8.1.1.4. Capital Circulante Líquido ou Capital de Giro (Ativo Circulante - Passivo Circulante) de, no mínimo, 10% (dez por cento) do valor estimado da contratação acima, tendo por base o balanço patrimonial e as demonstrações contábeis do último exercício social.

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

8.1.1.6. 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.

8.1.1.7. Justifica-se a exigência de requisitos de qualificação econômico-financeira, uma vez que a contratação de fornecedor financeiramente não qualificado impõe alto risco à Administração, pois em caso de eventual incapacidade do fornecedor no gerenciamento e pagamento das despesas decorrentes da mão de obra e demais insumos necessários à execução dos serviços poderá comprometer a garantia e suporte especializado dos softwares de antivírus do CONTRATANTE e comprometer segurança de informação deste tribunal. Destaca-se que para referência da contratação foi utilizado apenas o valor de um grupo, considerando que este Tribunal irá homologar somente o lote de menor preço.

9 - LOCAL E PRAZO DE ENTREGA E EXECUÇÃO DOS SERVICOS

9.1. 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 , no prazo máximo de **10 (dez) dias úteis,** contados do recebimento da Ordem de Fornecimento.

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

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

9.1.3. Deverão ser iniciados os prazos de garantia e atualização das licenças, após a instalação e configuração das licenças.

9.2. Os serviços de desinstalação, instalação e configuração deverão ser executados, no prazo máximo de **22 (vinte e dois) dias úteis**, contados da entrega das licenças.

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

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

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

9.5. 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.

9.6. 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.

10 - ESPECIFICAÇÃO TÉCNICA

10.1. Especificação Técnica presente no Anexo I deste termo.

11 - GARANTIA TÉCNICA, ATUALIZAÇÃO E SERVIÇOS DE INSTALAÇÃO E DESINSTALAÇÃO

11.1. Garantia técnica e atualização

11.1.1. 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;

11.1.2. 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;

11.1.3. 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;

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

11.1.4.1. As atualizações de vacina deverão ser fornecidas independente de solicitação da CONTRATANTE.

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

11.1.4.3. Deverá permitir atualizações da engine do agente (software), assim como da base de

dados, padrões de comportamento e quaisquer outros elementos pertinentes à solução;

11.1.5. 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:

11.1.5.1. 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;

11.1.5.2. 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:

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

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

11.1.6. Os serviços descritos neste item, exceto os serviços descritos no item 11.1.4.1, 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;

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

11.2. Serviços de instalação e desinstalação

11.2.1. Serviço de Desinstalação

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

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

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

11.2.1.4. 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;

11.2.1.4.1. 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;

11.2.1.5. 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;

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

11.2.2. Serviço de instalação e configuração

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

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

11.2.2.3. 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;

11.2.2.4. 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;

11.2.2.5. 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;

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

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

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

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

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

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

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

11.2.2.10.2.1. Versão de cada módulo da solução instalado;

11.2.2.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

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

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

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

11.2.2.10.2.5.1. IND – Índice de instalação;

11.2.2.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

11.2.2.10.2.5.3. QLA – Quantidade licenças adquiridas;

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

12 - CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

12.1. A equipe de planejamento não vislumbrou a necessidade de exigências especiais em cumprimento dos critérios de sustentabilidade, observadas as regras estabelecidas nas normas vigentes relativas ao desenvolvimento sustentável nas licitações e contratações públicas, bem como o o Plano de Logística Sustentável da Justiça Federal da 1ª Região (RESOLUÇÃO PRESI 4/2016), em especial o disposto no Art. 3º da referida resolução e o Art. 17 da Resolução Nº 201/2015, considerando que o objeto pretendido não envolve entrega de produtos ou bens por meio físico, bem como não há alocação de mão de obra residente nas instalações do Tribunal e os serviços serão prestados quase sempre pela via remota.

13 - OBRIGAÇÕES DA CONTRATADA

13.1. Obedecer aos prazos estabelecidos neste Termo de Referência e em seus anexos.

13.2. Fornecer, no prazo de 10 (dez) dias úteis, contados a partir da data de recebimento da ordem de fornecimento, por meio do endereço eletrônico para: TRF1 - sesei@trf1.jus.br; SJMG - nutec.mg@trf1.jus.br; e UFT -nati@uft.edu.br, as licenças da solução de antivírus nas versões mais recentes e compatíveis com o parque computacional da JF1.

13.3. A CONTRATADA deverá fornecer toda a documentação técnica original, completa e atualizada, contendo os manuais e guias de instalação, podendo ser em meio eletrônico.

13.4. Implantar a solução nos prazos constantes no item 09 deste termo.

13.5. Iniciar a prestação dos serviços de suporte técnico imediatamente após emissão do Termo de Recebimento Definitivo do fornecimento e instalação de licenças.

13.6. Ministrar o treinamento no prazo máximo de 10 dias úteis do inicio do treinamento.

13.7. Implementar no ambiente da CONTRATANTE, as evoluções tecnológicas necessárias para execução dos serviços contratados.

13.8. Garantir a qualidade do software em suas características operacionais, de manutenção, desempenho e consumo de hardware, durante o período de suporte.

13.9. Arcar com todos os custos, tributos e encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, taxas e outras despesas incidentes ou necessárias à perfeita execução do objeto desta contratação.

13.10. Comunicar ao Contratante, por escrito, quando verificar condições inadequadas ou a iminência de fatos que possam prejudicar a perfeita prestação do serviço.

13.11. Prestar informações e/ou esclarecimentos que venham ser solicitados pelo CONTRATANTE, referente a qualquer problema detectado ou andamento das atividades.

13.12. Manter, durante toda a execução do contrato, as condições de habilitação e qualificação exigidas para a contratação.

13.13. Apresentar, no prazo estabelecido pelo CONTRATANTE, o Termo de Compromisso assinado, conforme Anexo III.

13.14. Responsabilizar-se, sem qualquer espécie de solidariedade por parte do CONTRATANTE, pelas obrigações de natureza fiscal, previdenciária, trabalhista, acidentária e civil, em relação aos profissionais que forem alocados para a prestação dos serviços objeto do Contrato, ainda que verificados nas dependências do CONTRATANTE.

13.15. Responder por quaisquer prejuízos que seus técnicos causarem ao patrimônio no âmbito do Tribunal ou a terceiros, decorrentes de ação ou omissão culposa, procedendo imediatamente aos reparos e/ou indenizações cabíveis e assumindo o ônus decorrente.

13.16. 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.

13.17. Cumprir, às suas expensas, todas as cláusulas contratuais que definam suas obrigações.

13.18. 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 no Contrato e seus anexos.

13.19. 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.

13.20. Cumprir a execução dos serviços e atualização de versões, sempre que necessário, em tempo, forma e regime de horário devidamente estabelecidos pelo CONTRATANTE.

13.21. Garantir ao CONTRATANTE que o conjunto de software licenciado para uso não infrinja quaisquer patentes, direitos autorais.

13.22. Promover, em no máximo 5 (cinco) dias úteis, substituições das licenças, em caso de falhas ou erros que impossibilitem as instalações dos conjuntos de software, respeitadas as condições normais de uso.

13.23. 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.

13.24. A CONTRATADA, nos casos em que foram detectados vírus novos, cujas vacinas existentes não sejam eficazes, deverá ser apresentada solução de contorno, até a liberação de uma nova vacina específica para o caso.

13.25. Comunicar formal e imediatamente ao TRF1, todas as ocorrências anormais que possam comprometer a execução do serviço contratado.

13.26. A contratada deverá disponibilizar profissionais qualificados para realização do suporte técnico e curso de capacitação, conforme exigência contidas no Anexo I.

13.27. 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.

13.28. Deverá apresentar no prazo de 10 (dez) dias, após a assinatura do contrato, o cronograma de execução da implantação da solução (desinstalação da solução em uso no TRF1 e Seções e Subseções Judiciárias e instalação da nova solução), observados os prazos máximos de definidos neste termo.

13.29. Durante a prestação do suporte técnico on site, a licitante deverá se responsabilizar 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.

13.30. A CONTRATADA deverá 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 TRF1.

13.31. 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.

13.32. A CONTRATADA deverá informar ao CONTRATANTE o número do telefone para fins de esclarecimento de dúvidas relativas aos itens licitados, assim como para orientação e acompanhamento da solução de problemas quando não for demandada a presença de um técnico, a critério do CONTRATANTE.

13.33. Deverá ser informada página na Internet, do fabricante do(s) software(s), onde estejam disponíveis, 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).

13.34. A CONTRATADA deverá possibilitar ao CONTRATANTE fazer quaisquer ajustes de configuração em quaisquer funcionalidades da solução ofertada, para adequação ao ambiente onde está instalado, sem prejuízo dos serviços de suporte. 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 TRF1.

13.35. 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 TRF1 atualizada, de acordo com os padrões do FABRICANTE.

13.36. A CONTRATADA deverá manter a solução em funcionamento pelo período de 06 meses após o vencimento do contrato, período considerado como de transição ou renovação, sem custo para o CONTRATANTE, durante esse período não será exigido as funcionalidades de EDR, Sandbox e atualização dos componentes.

14 - OBRIGAÇÕES DO CONTRATANTE

14.1. Designar servidor ou comissão para acompanhar e fiscalizar o contrato.

14.2. Emitir Ordem de Fornecimento das licenças(Desinstalação e instalação), conforme prazo estabelecido no subitem 9 deste Termo.

14.3. Emitir Ordem de Execução dos Serviços (Treinamento) conforme prazo estabelecido no subitem 9 deste Termo.

14.4. Convocar os representantes da CONTRATADA para realização de reunião inicial, para alinhamento de expectativas contratuais.

14.5. Atestar o recebimento da solução e da prestação dos serviços fornecidos pela CONTRATADA, que estejam em conformidade com as especificações e prazos definidos neste Termo, conforme inspeções realizadas.

14.6. Recusar o recebimento do objeto que não estiver em conformidade com as especificações constantes da proposta apresentada pela CONTRATADA.

14.7. Avaliar relatório e estatísticas dos serviços executados pela CONTRATADA, observando as metas de níveis mínimos de serviço.

14.8. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável.

14.9. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato.

14.10. Comunicar à CONTRATADA qualquer irregularidade verificada na execução do contrato, determinando, de imediato, as providências necessárias a sua regularização.

14.11. Acompanhar e fiscalizar, rigorosamente, o cumprimento deste Termo.

14.12. Exigir, sempre que necessário, a apresentação da documentação pela CONTRATADA que comprove a manutenção das condições de habilitação que ensejaram a sua contratação.

14.13. Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA, necessários à execução do objeto.

14.14. 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 1 (um) mês, contado do recebimento pelo Contratante, podendo ser prorrogado, motivadamente, por igual período

14.15. Disponibilizar cópia de normas de segurança da informação e das demais normas pertinentes à execução dos serviços.

14.16. 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.

14.17. 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;

14.18. Comunicar à CONTRATADA eventuais alterações de tecnologias citadas neste termo ou em uso no TRF1.

14.19. Fornecer os acessos necessários para que a CONTRATADA possa realizar a devida instalação da solução adquirida.

14.20. As decisões e providências que ultrapassarem a competência do Executor do Contrato deverão ser solicitadas à autoridade competente, em tempo hábil, para a adoção das medidas cabíveis.

14.21. O gestor do Contrato deverá comunicar à autoridade superior, em tempo hábil e por escrito, as situações que impliquem em atraso e descumprimento de cláusulas contratuais, para adoção dos procedimentos necessários à aplicação das sanções contratuais cabíveis, resguardados os Princípios do

Contraditório e da Ampla Defesa, bem como as situações que impliquem em prorrogações/alterações contratuais, para autorização e demais providências visando a celebração do termo aditivo.

15 - RECEBIMENTO PROVISÓRIO E DEFINITIVO

15.1. Recebimento da Solução:

15.1.1. Para os itens 1, 2, 5 e 6 do objeto o recebimento se dará da seguinte forma:

15.1.1.1. Provisoriamente, no prazo máximo de 10 (dez) dias úteis, após a entrega das licenças, por Ordem de Fornecimento, mediante Termo de Recebimento Provisório.

15.1.1.1.1. 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 1 mil estações de trabalho distribuídas em pelo menos 3 seccionais 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.

15.1.1.1.2. Caso seja identificado problema ou pendência na solução, o CONTRATANTE notificará a CONTRATADA e o prazo para o recebimento provisório estabelecido no item 15.1.1.1. 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.

15.1.1.2. Definitivamente, no prazo máximo de 10 (dez) dias úteis, contados do término da instalação e configuração da solução em todo o ambiente da JF1, mediante Termo de Recebimento Definitivo assinado pelas partes.

15.1.1.2.1. O recebimento definitivo consiste na verificação do atendimento aos requisitos técnicos da solução e sua integral operabilidade no ambiente do JF1.

15.1.1.2.2. Caso seja identificado problema ou pendência na solução, o CONTRATANTE notificará a CONTRATADA e o prazo para o recebimento definitivo estabelecido no item 15.1.1.2. 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.

15.1.1.3. A solução poderá ser recusada nos seguintes casos:

15.1.1.3.1. Quando entregue com especificações técnicas inferiores ou divergentes das contidas neste termo de referência;

15.1.1.3.2. Quando identificado avarias ou defeitos.

15.1.2. Para o item 3 e 7 do objeto o recebimento se dará da seguinte forma:

15.1.2.1. Definitivamente, no prazo máximo de de 15 (quinze) dias corridos, contados a partir do 1º dia útil subsequente ao recebimento do documento de cobrança.

15.1.2.1.1. 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.

15.1.2.1.2. Os serviços poderão ser recusados no todo ou em parte nos seguintes casos:

15.1.2.1.2.1. Quando não foram atingidos os níveis mínimos de serviço ou quando não forem atendidos os requisitos estabelecidos no contrato e em seus anexos;

15.1.2.1.2.2. Quando identificados defeitos ou outras inconformidade.

15.1.3. Para o item 4 e 8 do objeto o recebimento se dará da seguinte forma:

15.1.3.1. Provisoriamente, no prazo máximo de 15 (quinze) dias corridos após o encerramento da Ordem de Execução dos Serviços, mediante Termo de Recebimento

Provisório.

15.1.3.2. Definitivamente, no prazo máximo de de 15 (quinze) dias corridos, contados a partir da data de assinatura do Termo de Recebimento Provisório.

15.1.3.3. Os serviços poderão ser recusados no todo ou em parte nos seguintes casos:

15.1.3.3.1. Quando não foram atingidos os níveis mínimos de serviço ou quando não forem atendidos os requisitos estabelecidos no contrato e em seus anexos;

15.1.3.3.2. Quando identificados defeitos ou outras inconformidade.

15.2. Procedimentos de Teste e Inspeção

15.2.1. Não se aplica, pois não será exigida amostra da solução, por ser tal exigência incompatível com o objeto da contratação e totalmente suprida pela exigência de apresentação do formulário de avaliação técnica da solução ofertada, conforme modelo constante do Anexo IV deste Termo.

15.3. Níveis Mínimos de Serviço Exigidos e Glosas aplicáveis

15.3.1. 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 da 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 = <u>TEX – TEST</u>** Onde: **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 quanto 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 da 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.	

16. GARANTIA CONTRATUAL

16.1. Será necessária a apresentação de garantia contratual de 5% (cinco por cento) do valor total do contrato, nos termos previstos na Lei 8.666/1993.

17 - PAGAMENTO

17.1. O pagamento será efetuado, até o 15º (décimo quinto) dia útil, a contar da data do atesto do documento de cobrança, devidamente protocolado no setor competente do CONTRATANTE.

17.2. O atesto ocorrerá da seguinte forma:

17.2.1. Para os itens 1, 2, 5 e 6 do objeto:

17.2.1.1. 1ª atesto - 30% (sessenta por cento) após o recebimento provisório, por ordem de fornecimento;

17.2.1.2. 2ª atesto - 70% (quarenta por cento) após o recebimento definitivo.

17.2.1.3. A forma de pagamento se justifica pela restrição orçamentária para o próximo exercício, vale destacar que por experiencia da JF1 esse tipo de solução dificilmente apresenta algum tipo de falha e sua garantia terá início a partir do recebimento definitivo.

17.2.2. Para o item 3 e 7 do objeto o serviços serão atestados mensalmente, no prazo estabelecido no subitem 7.1.2.1. deste Termo.

17.2.3. Para o item 4 e 8 do objeto o serviços serão atestados por ordem de execução de serviço, no prazo estabelecido no subitem 15. deste Termo.

17.3. Deverá constar do documento de cobrança o número do contrato firmado com o CONTRATANTE.

17.4. A CONTRATADA deverá comprovar, para fins de pagamento, a regularidade perante o Fundo de Garantia do Tempo de Serviço – FGTS (Certificado de Regularidade de Situação do FGTS – CRF), quanto à Receita Federal e Dívida Ativa da União (Certidão Conjunta de Débitos relativos às Tributos Federais e à Dívida Ativa da União).

17.5. Poderá ser dispensada a apresentação dos referidos documentos, se confirmada sua validade em consulta online ao SICAF – Sistema Unificado de Cadastramento de Fornecedores.

17.6. 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.

17.7. 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.

17.8. 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.

17.9. Os pagamentos estarão sujeitos à retenção na fonte dos tributos, conforme legislação vigente.

18 - SANÇÕES ADMINISTRATIVAS

18.1. 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. 28 do Decreto 5.450/2005).

18.2. A penalidade fundada em comportamento ou conduta inidônea ensejará impedimento de licitar e de contratar com a União, Estados, Distrito Federal ou Municípios e descredenciamento no SICAF, pelo prazo de até 05 (cinco) anos, na forma do disposto no art. 7º da Lei 10.520/2002.

18.3. As sanções previstas nas alíneas “a” e “c” do subitem 18.1. desta cláusula poderão ser aplicadas com a da alínea “b” do mesmo subitem.

18.4. Caso a empresa vencedora se recuse a anexar proposta de preços ou assinar a Ata de Registro de Preços no prazo indicado, sem motivo justificado, ficará caracterizado o descumprimento total da obrigação. Em consequência, ser-lhe-á aplicada a multa prevista na alínea "b" do subitem 18.1., no percentual de 10% sobre o valor de sua proposta, podendo ser cumulada com a sanção prevista na alínea "c" do subitem 18.1.

18.5. O atraso injustificado na entrega do objeto desta contratação ou qualquer outro inadimplemento contratual, com exceção das previstas nos subitens 15.3.1, 18.6 e 18.9 desta cláusula, sujeitará a contratada à multa de 0,5% (cinco décimos por cento) por dia de atraso, sobre o valor correspondente à parte entregue com atraso, até o limite de 10 (dez) dias corridos.

18.5.1. A partir do 11º dia, a multa diária 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 18.5.

18.6. O descumprimento dos prazos de atendimento dos chamados por parte da Contratada, por período superior ao previsto no subitem 15.3.1. deste Termo, 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.

18.6.1. 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 18.6.

18.7. 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 fará incidir a sanção prevista no subitem 18.5.

18.8. 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.

18.9. Se em decorrência de ação ou omissão, pela Contratada, o cumprimento da obrigação inadimplida tornar-se inútil em momento posterior, a Contratada estará sujeita à multa de 0,5% (cinco décimos por cento) sobre o valor total do contrato e por ocorrência, sem prejuízos das demais cominações contratuais e legais aplicáveis.

18.10. 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.

18.11. 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.

18.12. 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.

18.13. 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 nos subitens 18.5. e 18.6.

18.14. 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).

18.15. A aplicação de quaisquer das penalidades previstas neste instrumento será precedida de regular processo administrativo, assegurados o contraditório e a ampla defesa.

18.16. O Contratante promoverá o registro no SICAF de toda e qualquer penalidade imposta à

Contratada.

19 - DA VIGÊNCIA

19.1. O instrumento de contratual entra em vigor a partir de _____, tendo seu término previsto para _____.

19.2. Na vigência acima estabelecida estão inclusos os seguintes prazos:

19.2.1. Até 10 (dez) dias úteis, para a emissão e entrega da Ordem de Fornecimento, contados da data de assinatura do contrato, com término previsto para _____.

19.2.2. Até 10 (dez) dias úteis, para a disponibilização da solução, contados a partir do recebimento da Ordem de Fornecimento, com término previsto para _____.

19.2.3. Até 22 (vinte e dois) dias úteis, para o término dos serviços de desinstalação, instalação e configuração, contados a partir da entrega das licenças, com término previsto para _____.

19.2.4. Até 10 (dez) dias úteis, para emissão do Termo de Recebimento Provisório da solução, contados da entrega das licenças, com término previsto para _____.

19.2.5. 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 da JF1, com término previsto para _____.

19.2.6. Até 60 (sessenta) meses de vigência da garantia técnica, contados a partir do recebimento definitivo da solução, com término previsto para _____.

19.2.7. Até 12 (doze) meses de vigência do suporte especializado, contados a partir do recebimento definitivo da solução, com término previsto para _____.

19.2.7.1. O suporte especializado poderá ser prorrogado por períodos iguais e sucessivos, limitado a 60 (sessenta) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do Inciso II, Art. 57, da Lei nº 8.666, de 1993.

19.2.8. Até 10 (dez) dias úteis, para inicio do treinamento, contados a partir do recebimento da ordem de execução do serviço, com término previsto para _____.

19.2.9. Até 10 (dez) dias úteis, para finalização do treinamento, contados a partir do inicio do treinamento, com término previsto para _____.

20. DOS REQUISITOS DE SEGURANÇA

20.1. A solução deve adequar-se às necessidades de negócio e técnicas estabelecidas pela segurança do Tribunal. É necessário considerar a infraestrutura existente, bem como sua integração eficiente.

20.2. Para a formalização desta contratação, faz-se necessário que seja exigida a assinatura do compromisso de confidencialidade de informações que eventualmente sejam trocadas entre Fornecedor e TRF1, conforme modelo constante no Anexo III deste Termo. Tal termo deve exigir manifestação da contratada quanto à guarda, privacidade e o sigilo das informações que venham a ter conhecimento em razão do exercício de suas atividades bem como das informações disponibilizadas pela entidade contratante.

20.3. Na execução do objeto, devem ser observados os ditames da Lei 13.709/2018 (Lei Geral de Proteção de Dados) – LGPD, notadamente os relativos às medidas de segurança e controle para proteção dos dados pessoais a que tiver acesso mercê da relação jurídica estabelecida, mediante adoção de boas práticas e de mecanismos eficazes que evitem acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados.

20.4. A contratada obriga-se a dar conhecimento formal a seus prepostos, empregados ou colaboradores das disposições relacionadas à proteção de dados e a informações sigilosas, na forma da Lei 13.709/2018 (LGPD), da Resolução/ CNJ 363/2021 e da Lei 12.527/2011.

> **20.4.1.** Obriga-se também a comunicar à Administração, em até 24 (vinte e quatro) horas, 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).

20.5. O tratamento de dados pessoais dar-se-á de acordo com os princípios e as hipóteses previstas nos arts. 6º, 7º e 11 da Lei 13.709/2018 (LGPD), limitado ao estritamente necessário à consecução do objeto, na forma deste instrumento e seus anexos.

20.6. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal, bem como deverão ser observadas as disposições legais previstas na Lei 13.709/18 (LGPD) e Resolução CNJ 363/2021 que Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.

20.7. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoas sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento da ata de registro de preços.

20.8. As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD.

20.9. A LICITANTE, declara que tem ciência da existência da Lei Geral de Proteção de Dados (LGPD) e, se compromete a adequar todos os procedimentos internos ao disposto na legislação, com intuito de proteção dos dados pessoais repassados pelo TRF1.

20.10. A LICITANTE, fica obrigada a comunicar ao TRF1, em até 24 (vinte e quatro) horas, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD.

20.11. Os dados pessoais serão eliminados pela Contratada após o término de seu tratamento ou a pedido do TRF1, no âmbito e nos limites técnicos das atividades, podendo ser autorizado pelo TRF1 sua conservação conforme hipóteses previstas na Lei Lei 13.709/18 (LGPD).

20.12. Para presente contratação não há tratamento específico de dados pessoais.

21 - DO VALOR ESTIMADO DA CONTRATAÇÃO

21.1. Procedimento para Levantamento de Custos:

21.1.1. Inicialmente, cumpre informar que foram realizadas pesquisas no Painel de Preços e Banco de Preços conforme documentos (14543964 e 14543977), cujo contratações similares localizadas não pudessem ser utilizados como referência na pesquisa, sendo utilizado o preço público do TSE - ARP 01/2022 (16125645) e quatro propostas comerciais de fornecedores (16129805, 16129811, 16129818 e 16129829).

21.1.2. Os custos para a contratação obedecem a adoção da **MÉDIA** como valor estimado para os itens 1, 2, 5 e 6 e **MENOR PREÇO** para os itens 3, 4, 7 e 8 conforme justificativas descritas na Informação Conclusiva - Valor Estimado da Licitação (16142042), bem como consta no Mapa Comparativo de Preços (16129908).

21.1.3. Na pesquisa de preços foi cumprida a recomendação contida no Acórdão 1.445/2015-Plenário, quanto à hierarquia de consulta, tendo sido consultado primeiro Painel de Preços do Governo Federal, contratações públicas similares e bancos de preços, atendendo assim as regras previstas na Instrução Normativa nº 73/2020. **Dessa forma a equipe se manifesta pela exequibilidade do valor estimado**.

21.1.4. Destarte, seguem abaixo os valores estimados para a presente contratação, em que será o valor apenas de **1 GRUPO**, visto que será contratado apenas o grupo que restar mais econômico pra administração.

GRUPO	ITEM	DESCRIÇÃO DOS BENS E SERVIÇOS	UNIDADE DE MEDIDA	QTDS ESTIMADAS			CUSTO UNITÁRIO	CUSTO TOTAL
				POR ÓRGÃO		TOTAL		
1	1	Solução de antivírus com licenciamento perpétuo, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1	12.784	19.284	211,46	4.077.794,64
				SJMG	3.500			
				UFT	3.000			
	2	Solução de antivírus com licenciamento perpétuo, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1	2.472	3.122	227,96	711.691,12
				SJMG	450			
				UFT	200			
	3	Serviço de suporte técnico especializado	Meses	TRF1	12	36	11.900,00	428.400,00
				SJMG	12			
				UFT	12			
	4	Treinamento	Alunos	TRF1	10	26	1.716,56	44.630,56
				SJMG	6			
				UFT	10			
VALOR TOTAL DO GRUPO 1								**5.262.516,32**
	5	Solução de antivírus com licenciamento por meio de subscrição, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1	12.784	19.284	211,46	4.077.794,64
				SJMG	3.500			
				UFT	3.000			
		Solução de antivírus		TRF1	2.472			

2	6	com licenciamento por meio de subscrição, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses	Licença	SJMG UFT	450 200	3.122	227,96	711.691,12
	7	Serviço de suporte técnico especializado	Meses	TRF1 SJMG UFT	12 12 12	36	11.900,00	428.400,00
	8	Treinamento	Alunos	TRF1 SJMG UFT	10 6 10	26	1.716,56	44.630,56
VALOR TOTAL DO GRUPO 2								**5.262.516,32**

22 - EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Luiz Alberto Lima da Costa

Integrante Requisitante

Rodrigo Alves Migueleti

Integrante Técnico

Paulo de Tarso de Almada Santos

Integrante Técnico

Cristina Kelly Fritsch

Integrante Administrativo

ANEXO I
ESPECIFICAÇÕES TÉCNICAS

1. SOLUÇÃO DE ANTIVÍRUS PARA ESTAÇÕES DE TRABALHO LICENÇA PERPÉTUA

1.1. Características gerais:

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;

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

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;

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

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 ANEXO II;

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

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;

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

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;

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

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;

1.2. Gerenciamento centralizado:

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);

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;

1.2.3. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no ANEXO II;

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

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

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;

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;

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

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;

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;

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

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

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;

1.2.11.3. Deverá permitir criação de alertas e notificação de eventos para

administradores e usuários determinados;

1.2.11.4. Deverá possibilitar pesquisa no histórico de eventos;

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

1.2.12. Deverá disponibilizar as seguintes consultas pré-definidas:

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

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

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

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

1.2.12.5. Versões dos produtos instalados;

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

1.2.13. Deverá permitir criação de dashboards;

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

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.

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;

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;

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);

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

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;

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:

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.

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

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

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

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

1.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura

hierárquica da JF1 ou pontos específicos;

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

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

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;

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.

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

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

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);

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

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

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;

1.2.32. As atualizações deverão ser do tipo incremental;

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

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

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

1.2.35. Deverá possibilitar restauração manual de arquivos quarentenados;

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

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;

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

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;

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

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.

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

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

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

1.3. Serviço de Desinstalação

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

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

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

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;

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;

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;

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

1.4. Serviço de instalação e configuração

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

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

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;

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;

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;

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

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

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

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

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

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

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

1.4.10.2.1. Versão de cada módulo da solução instalado;

1.4.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

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

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

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:

1.4.10.2.5.1. IND – Índice de instalação;

1.4.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

1.4.10.2.5.3. QLA – Quantidade licenças adquiridas;

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;

1.5. Solução de antivírus para estações de trabalho

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

1.5.1.1. Windows 8.1;

1.5.1.2. Windows 10;

1.5.1.3. Linux CentOS;

1.5.1.4. Linux Debian;

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

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;

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;

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

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

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

1.5.6. Deverá possuir mecanismo de análise comportamental;

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

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

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;

1.5.10. Deverá permitir criar bloqueios personalizados, baseado no nome do aplicativo,

caminho do aplicativo e hash do arquivo;

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

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 1.5.1;

1.5.13. Deverá possuir proteção contra BOTs e variantes;

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

1.5.14.1. Processos suspeitos deverão ser bloqueados;

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;

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

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

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

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

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;

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

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;

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

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

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

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;

1.5.27. Deverá oferecer proteção para alterações suspeitas de registro;

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

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

1.5.30. Deverá oferecer proteção contra-ataques direcionados;

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

1.5.32. Deverá permitir inclusão de exceções aplicações e caminhos;

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

1.5.33.1. Na memória principal (RAM);

1.5.33.2. Em arquivos;

1.5.33.3. No tráfego de rede;

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

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

1.5.33.6. Em processos de inicialização automática;

1.5.33.7. Em serviços criados/modificados;

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

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;

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;

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

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

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;

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;

1.5.40. Deverá oferecer mecanismo de controle de dispositivos externos;

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

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:

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

1.5.42.2. Transferências de dados para dispositivos mobile.;

1.5.42.3. Transferências de dados para dispositivos de armazenamento externos;

1.5.42.4. Possibilitar ações de bloqueio na execução de arquivos que possam ser carregados por upload em browsers e clientes de e-mail.

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;

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;

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

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

1.5.45.2. Recebimento de políticas e tarefas da gerência;

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;

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

1.5.45.4.1. Nome da ameaça;

1.5.45.4.2. Tipo da ameaça;

1.5.45.4.3. Arquivo ou local infectado;

1.5.45.4.4. Data e hora da detecção;

1.5.45.4.5. Mecanismo que gerou a detecção;

1.5.45.4.6. Nome da máquina/endereço IP;

1.5.45.4.7. Ação realizada;

1.5.45.4.8. Usuário logado no sistema;

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

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;

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;

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

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

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;

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;

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;

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

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

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;

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;

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:

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;

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:

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;

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.

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;

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.

2. SOLUÇÃO DE ANTIVIRUS PARA SERVIDORES LICENÇA PERPÉTUA

2.1. Características gerais:

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;

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

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;

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

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 ANEXO II;

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

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;

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

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;

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

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;

2.2. Gerenciamento centralizado:

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);

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;

2.2.3. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no ANEXO II;

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

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

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;

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;

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

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;

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;

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

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

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;

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

2.2.11.4. Deverá possibilitar pesquisa no histórico de eventos;

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

2.2.12. Deverá disponibilizar as seguintes consultas pré-definidas:

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

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

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

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

2.2.12.5. Versões dos produtos instalados;

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

2.2.13. Deverá permitir criação de dashboards;

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

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

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;

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;

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);

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

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;

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:

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.

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

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

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

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

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

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

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

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;

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.

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

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

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);

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

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

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;

2.2.32. As atualizações deverão ser do tipo incremental;

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

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

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

2.2.35. Deverá possibilitar restauração manual de arquivos quarentenados;

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

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;

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

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;

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

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.

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

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

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

2.3. Serviço de Desinstalação

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

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

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

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;

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;

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;

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

2.4. Serviço de instalação e configuração

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

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

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;

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;

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;

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

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

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

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

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

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

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

2.4.10.2.1. Versão de cada módulo da solução instalado;

2.4.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

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

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

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:

2.4.10.2.5.1. IND – Índice de instalação;

2.4.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

2.4.10.2.5.3. QLA – Quantidade licenças adquiridas;

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;

2.5. Solução de antivírus para equipamentos servidores

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

2.5.1.1. Windows Server 2012;

2.5.1.2. Windows Server 2016;

2.5.1.3. Windows Server 2019 e posteriores;

2.5.1.4. Linux CentOS;

2.5.1.5. Linux Debian;

2.5.1.6. Linux Red Hat;

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

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;

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;

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

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

2.5.6. Deverá possuir mecanismo de análise comportamental;

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

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

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

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

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 2.5.1;

2.5.12. Deverá possuir proteção contra BOTs e variantes;

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

2.5.13.1. Processos suspeitos deverão ser bloqueados;

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;

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

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

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

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

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;

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

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;

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;

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

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.

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

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

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;

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

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

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

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;

2.5.29. Deverá oferecer proteção para alterações suspeitas de registro;

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

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

2.5.32. Deverá oferecer proteção contra ataques direcionados;

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

2.5.34. Deverá permitir inclusão de exceções aplicações e caminhos;

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

2.5.35.1. Na memória principal (RAM);

2.5.35.2. Em arquivos;

2.5.35.3. No tráfego de rede;

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

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

2.5.35.6. Em processos de inicialização automática;

2.5.35.7.Em serviços criados/modificados;

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

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;

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

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

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;

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;

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;

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;

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

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

2.5.43.2. Recebimento de políticas e tarefas da gerência;

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;

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

2.5.43.4.1. Nome da ameaça;

2.5.43.4.2. Tipo da ameaça;

2.5.43.4.3. Arquivo ou local infectado;

2.5.43.4.4. Data e hora da detecção;

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

2.5.43.4.6. Nome da máquina/endereço IP;

2.5.43.4.7. Ação realizada;

2.5.43.4.8. Usuário logado no sistema;

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

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;

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;

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

2.6. Garantia e atualização das licenças, para servidores

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;

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;

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;

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

2.6.5. As atualizações deverão ser fornecidas independente de solicitação da

CONTRATANTE.

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;

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;

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:

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;

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:

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;

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.

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;

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.

3. SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO

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.

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

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:

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;

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:

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;

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;

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.

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

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.

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

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.

4. TREINAMENTO

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

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

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

4.1.3. Instalação e configuração dos componentes da gerência.

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

4.1.5. Instalação e configuração dos agentes.

4.1.6. Criação e execução de consultas e relatórios

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

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

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

4.5. O treinamento deverá ser realizado por videoconferência.

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

4.6.1. Nome da empresa que ministrou a capacitação;

4.6.2. Nome do curso;

4.6.3. Nome do servidor capacitado;

4.6.4. Data de início e término da capacitação;

4.6.5. Carga horária;

4.6.6. Conteúdo programático.

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

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:

4.8.1. Pontualidade;

4.8.2. Didática do instrutor;

4.8.3. Eficiência no repasse do conteúdo;

4.8.4. Adequação do treinamento ao conteúdo exigido no item 4.1;

4.8.5. Adequação da carga horária.

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.

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.

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

5. SOLUÇÃO DE ANTIVÍRUS PARA ESTAÇÕES DE TRABALHO SUBSCRIÇÃO

5.1. Características gerais:

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;

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

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;

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

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 ANEXO II;

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

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;

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

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

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

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;

5.2. Gerenciamento centralizado:

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);

5.2.2. 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;

5.2.3. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no ANEXO II;

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

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

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;

5.2.7. 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;

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

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;

5.2.10. 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;

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

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

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;

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

5.2.11.4. Deverá possibilitar pesquisa no histórico de eventos;

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

5.2.12. Deverá disponibilizar as seguintes consultas pré-definidas:

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

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

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

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

5.2.12.5. Versões dos produtos instalados;

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

5.2.13. Deverá permitir criação de dashboards;

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

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.

5.2.15. 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;

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;

5.2.17. 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);

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

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;

5.2.20. 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:

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

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

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

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

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

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

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

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

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;

5.2.25. 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.

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

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

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);

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

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

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;

5.2.32. As atualizações deverão ser do tipo incremental;

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

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

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

5.2.35. Deverá possibilitar restauração manual de arquivos quarentenados;

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

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;

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

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;

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

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.

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

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

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

5.3. Serviço de Desinstalação

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

5.3.2. A CONTRATANTE deverá fornecer as credenciais necessárias para a execução da

desinstalação, como usuário com privilégio.

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

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;

5.3.4.1. 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;

5.3.5. 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;

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

5.4. Serviço de instalação e configuração

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

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

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;

5.4.4. 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;

5.4.5. 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;

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

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

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

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

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

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

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

5.4.10.2.1. Versão de cada módulo da solução instalado;

5.4.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

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

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

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:

5.4.10.2.5.1. IND – Índice de instalação;

5.4.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

5.4.10.2.5.3. QLA – Quantidade licenças adquiridas;

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. Solução de antivírus para estações de trabalho

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

5.5.1.1. Windows 8.1;

5.5.1.2. Windows 10;

5.5.1.3. Linux CentOS;

5.5.1.4. Linux Debian;

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

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;

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

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

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

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

5.5.6. Deverá possuir mecanismo de análise comportamental;

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

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

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;

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

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

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 5.5.1;

5.5.13. Deverá possuir proteção contra BOTs e variantes;

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

5.5.14.1. Processos suspeitos deverão ser bloqueados;

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;

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

5.5.17. Deverá oferecer tecnologia de proteção baseada em técnicas de Inteligência Artificial

do tipo Machine Learning;

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

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

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;

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

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;

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

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

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

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;

5.5.27. Deverá oferecer proteção para alterações suspeitas de registro;

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

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

5.5.30. Deverá oferecer proteção contra-ataques direcionados;

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

5.5.32. Deverá permitir inclusão de exceções aplicações e caminhos;

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

5.5.33.1. Na memória principal (RAM);

5.5.33.2. Em arquivos;

5.5.33.3. No tráfego de rede;

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

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

5.5.33.6. Em processos de inicialização automática;

5.5.33.7. Em serviços criados/modificados;

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

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;

5.5.36. 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;

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

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

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;

5.5.39. 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;

5.5.40. Deverá oferecer mecanismo de controle de dispositivos externos;

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

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:

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

5.5.42.2. Transferências de dados para dispositivos mobile.;

5.5.42.3. Transferências de dados para dispositivos de armazenamento externos;

5.5.42.4. Possibilitar ações de bloqueio na execução de arquivos que possam ser carregados por upload em browsers e clientes de e-mail.

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;

5.5.44. 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;

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

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

5.5.45.2. Recebimento de políticas e tarefas da gerência;

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;

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

5.5.45.4.1. Nome da ameaça;

5.5.45.4.2. Tipo da ameaça;

5.5.45.4.3. Arquivo ou local infectado;

5.5.45.4.4. Data e hora da detecção;

5.5.45.4.5. Mecanismo que gerou a detecção;

5.5.45.4.6. Nome da máquina/endereço IP;

5.5.45.4.7. Ação realizada;

5.5.45.4.8. Usuário logado no sistema;

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

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;

5.5.48. Deverá fornecer informações do status do agente e de seus componentes, através da

gerência com informações atualizadas com delay máximo de 5 minutos;

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

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

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;

5.6.2. 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;

5.6.3. 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;

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

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

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;

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

5.6.8. 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:

5.6.8.1. 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;

5.6.8.2. 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:

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

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

5.6.9. 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;

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

6. SOLUÇÃO DE ANTIVIRUS PARA SERVIDORES SUBSCRIÇÃO

6.1. Características gerais:

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;

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

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;

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

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 ANEXO II;

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

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;

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

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;

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

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;

6.2. Gerenciamento centralizado:

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);

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;

6.2.3. A gerência centralizada deverá estar em consonância e compatibilidade com o ambiente tecnológico exposto no ANEXO II;

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

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

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;

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;

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

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;

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;

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

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

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;

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

6.2.11.4. Deverá possibilitar pesquisa no histórico de eventos;

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

6.2.12. Deverá disponibilizar as seguintes consultas pré-definidas:

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

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

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

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

6.2.12.5. Versões dos produtos instalados;

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

6.2.13. Deverá permitir criação de dashboards;

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

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

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;

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;

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);

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

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;

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:

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.

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

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

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

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

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

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

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

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;

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.

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

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

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);

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

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

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;

6.2.32. As atualizações deverão ser do tipo incremental;

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

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

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

6.2.35. Deverá possibilitar restauração manual de arquivos quarentenados;

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

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;

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

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;

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

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.

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

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

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

6.3. Serviço de Desinstalação

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

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

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

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;

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;

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;

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

6.4. Serviço de instalação e configuração

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

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

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;

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;

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;

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

6.4.7. Deve permitir que se instale os agentes individualmente por computador ou em lote,

para vários computadores;

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

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

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

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

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

6.4.10.2.1. Versão de cada módulo da solução instalado;

6.4.10.2.2. Versão da DAT ou catálogo de vacinas instalado;

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

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

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:

6.4.10.2.5.1. IND – Índice de instalação;

6.4.10.2.5.2. QAI – Quantidade de computadores com antivírus instalado;

6.4.10.2.5.3. QLA – Quantidade licenças adquiridas;

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;

6.5. Solução de antivírus para equipamentos servidores

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

6.5.1.1. Windows Server 2012;

6.5.1.2. Windows Server 2016;

6.5.1.3. Windows Server 2019 e posteriores;

6.5.1.4. Linux CentOS;

6.5.1.5. Linux Debian;

6.5.1.6. Linux Red Hat;

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

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;

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;

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

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

6.5.6. Deverá possuir mecanismo de análise comportamental;

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

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

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

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

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 6.5.1;

6.5.12. Deverá possuir proteção contra BOTs e variantes;

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

6.5.13.1. Processos suspeitos deverão ser bloqueados;

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;

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

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

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

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

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;

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

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;

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;

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

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.

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

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

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;

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

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

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

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;

6.5.29. Deverá oferecer proteção para alterações suspeitas de registro;

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

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

6.5.32. Deverá oferecer proteção contra ataques direcionados;

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

6.5.34. Deverá permitir inclusão de exceções aplicações e caminhos;

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

6.5.35.1. Na memória principal (RAM);

6.5.35.2. Em arquivos;

6.5.35.3. No tráfego de rede;

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

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

6.5.35.6. Em processos de inicialização automática;

6.5.35.7.Em serviços criados/modificados;

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

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;

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

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

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;

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;

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;

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;

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

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

6.5.43.2. Recebimento de políticas e tarefas da gerência;

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;

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

6.5.43.4.1. Nome da ameaça;

6.5.43.4.2. Tipo da ameaça;

6.5.43.4.3. Arquivo ou local infectado;

6.5.43.4.4. Data e hora da detecção;

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

6.5.43.4.6. Nome da máquina/endereço IP;

6.5.43.4.7. Ação realizada;

6.5.43.4.8. Usuário logado no sistema;

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

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;

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;

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

6.6. Garantia e atualização das licenças, para servidores

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;

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;

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;

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

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

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;

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;

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:

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;

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:

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;

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.

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;

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.

7. SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO

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.

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

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:

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;

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:

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;

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;

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.

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

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.

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

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.

8. TREINAMENTO

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

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

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

8.1.3. Instalação e configuração dos componentes da gerência.

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

8.1.5. Instalação e configuração dos agentes.

8.1.6. Criação e execução de consultas e relatórios

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

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

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

8.5. O treinamento deverá ser realizado por videoconferência.

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

8.6.1. Nome da empresa que ministrou a capacitação;

8.6.2. Nome do curso;

8.6.3. Nome do servidor capacitado;

8.6.4. Data de início e término da capacitação;

8.6.5. Carga horária;

8.6.6. Conteúdo programático.

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

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:

8.8.1. Pontualidade;

8.8.2. Didática do instrutor;

8.8.3. Eficiência no repasse do conteúdo;

8.8.4. Adequação do treinamento ao conteúdo exigido no item 8.1;

8.8.5. Adequação da carga horária.

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.

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.

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

ANEXO II
AMBIENTE TECNOLÓGICO

1. Plataforma de Hardware e software

1.1. Sistemas operacionais utilizados em servidores:

1.1.1. Windows Server 2012 (64 bits) e superiores.

1.1.2. Linux Server (64 bits).

1.2. Software utilizados nas estações clientes:

1.2.1. Windows 8.1 e 10;

1.2.2. Antivírus McAfee.

1.3. Browsers de mercado:

1.3.1. Chrome;

1.3.2. Internet Explorer;

1.3.3. Mozilla Firefox;

1.3.4. Microsoft Edge.

1.4. Ambiente de virtualização:

1.4.1. VMware Vsphere;

1.4.2. Oracle Virtualization Machine;

1.4.3. Microsoft Hyper-V.

1.5. Ferramentas de backup:

1.5.1. NetBackup.

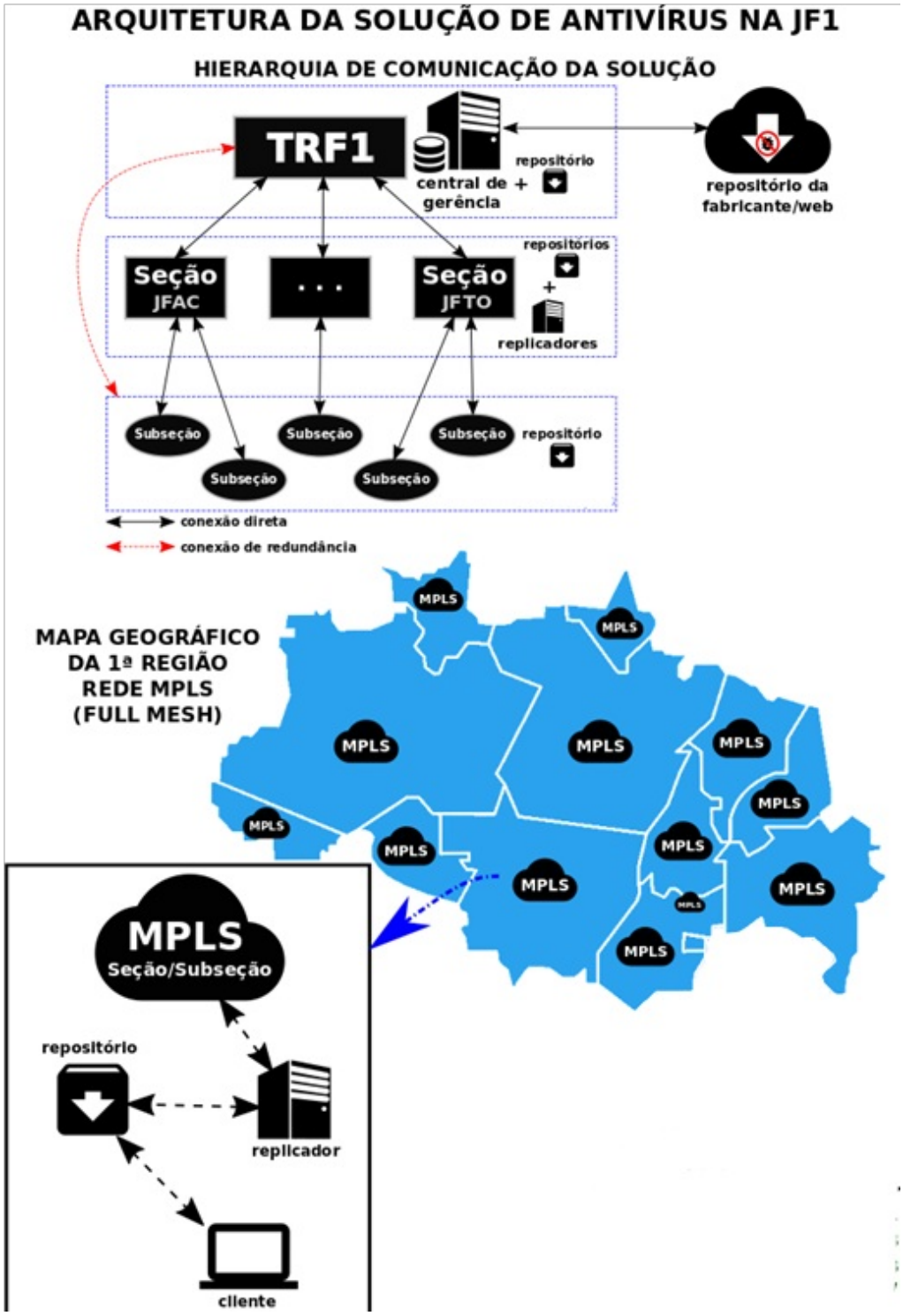
2. Informações gerais:

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

3. Ciclo de Vida:

3.1. O TRF1 procura adotar ciclo de vida de 5 (cinco) anos para todos os ativos de Datacenter.

4. Figura 1 - do Mapa Arquitetural:



ANEXO III
COMPROMISSO DE CONFIDENCIALIDADE DE INFORMAÇÕES

1. OBJETO

1.1. Este termo 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 sobre a proteção geral de dados.

2. CONCEITOS E DEFINIÇÕES

2.1. Para os efeitos deste Termo, 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 TERMO 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 Termo 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 termo 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 termo.

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 termo, 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 termo e 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 termo.

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.

6. DURAÇÃO DO SIGILO

6.1. O presente termo 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.

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 nº. 8.666/1993.

8. DISPOSIÇÕES GERAIS

8.1. Este termo 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 termo 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 termo 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 termo, 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 termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas.

Este termo 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.

TERMO DE CIÊNCIA

Contrato Número:

Objeto:

Gestor do Contrato: Matrícula:

Contratante:

Contratada: CNPJ:

Preposto da Contratada: CPF:

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o Termo de Compromisso de Manutenção de Sigilo e das normas de segurança vigentes no Contratante.

_____, _____ de _____ de 20____.

CIÊNCIA Contratada - Funcionários

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

(Nome e Matrícula):
_____

ANEXO IV

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.

EDITAL E DA ESPECIFICAÇÃO TÉCNICA	DOCUMENTO COMPROBATÓRIO (CATÁLOGO / FOLDER / MANUAL) COM INDICAÇÃO DA PÁGINA E CITAÇÃO DO CONTEÚDO COMPROBATÓRIO DO REQUISITO
ITEM 1 - SOLUÇÃO DE ANTIVÍRUS PARA ESTAÇÕES DE TRABALHO	
1.1...	
1.2....	
...	
ITEM 2 -SOLUÇÃO DE ANTIVIRUS PARA SERVIDORES	
2.1....	
2.2....	

ANEXO V

ORDEM DE FORNECIMENTO

PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO

IDENTIFICAÇÃO DA ORDEM DE FORNECIMENTO

NÚMERO DO CONTRATO:		**ORDEM DE FORNECIMENTO Nº:**	
PA Nº		**ARP Nº:**	
GESTOR DO CONTRATO:			
FORNECEDOR:			

AUTORIZAMOS O FORNECIMENTO DOS PRODUTOS ABAIXO DISCRIMINADOS MEDIANTE CONDIÇÕES CONSTANTES DO CONTRATO REFERIDO.

DADOS DO PRODUTO E LOCAIS DE ENTREGA

ITEM	PRODUTO	QTD.	LOCAL DE ENTREGA	CONTATO

DATAS E PRAZOS

ITEM	DATA LIMITE PARA ENTREGA	DATA DA ENTREGA

CIÊNCIA

DADOS DA AUTORIZAÇÃO

Data da emissão da Ordem de Fornecimento: XX/XX/XXXX

_____

Carimbo e assinatura do Gestor

Data de recebimento da Ordem de Fornecimento: XX/XX/XXXX

_____

Carimbo e assinatura da CONTRATADA

ANEXO VI
ORDEM DE EXECUÇÃO DE SERVIÇO

IDENTIFICAÇÃO DA ORDEM DE EXECUÇÃO DE SERVIÇO - OES

Número do Contrato:

Número da OES:

Motivo da OES:

Descrição da Solicitação:

Empresa CONTRATADA:

Data da OES:

Tipo da OES:

Nome do requisitante:

Contato do requisitante:

ESPECIFICAÇÃO DO SERVIÇO

Item do Contrato:

Local de prestação do serviço:

AUTORIZAÇÃO PARA A REALIZAÇÃO DO SERVIÇO

Nome do Solicitante: _____ Cargo/Função: _____ De Acordo: ___/____/____ _____ Assinatura/Carimbo	Nome do Responsável CONTRATADA: _____ Cargo/Função: _____ De Acordo: ___/____/____ _____ Assinatura/Carimbo

ATESTO DOS SERVIÇOS

Nome do Solicitante CONTRATANTE:_____ Cargo/Função:_____ Telefone / e-mail:_____ Avaliação dos níveis de serviço: _____ Glosas: _____ De Acordo: ___/____/____ _____ Assinatura(s)/Carimbo(s)	Nome do Responsável Técnico da CONTRATADA:_____ Telefone / e-mail:_____ De Acordo: ___/____/____ _____ Assinatura/Carimbo

ANEXO VII

MODELO DE PROPOSTA

Ao

Tribunal Regional Federal da 1º Região - TRF1

Ref.: Pregão Eletrônico nº ____/2022

Prezados Senhores,

A Empresa _____, inscrita no CNPJ nº _____, inscrição estadual nº _____ estabelecida no _____, neste ato representado por seu Representante Legal o Sr. _____, vem apresentar proposta de preços de conformidade com as especificações a seguir.

Objeto: _____.

GRUPO	ITEM	DESCRIÇÃO DOS BENS E SERVIÇOS	UNIDADE DE MEDIDA	QTDS ESTIMADAS			CUSTO UNITÁRIO	CUSTO TOTAL
				POR ÓRGÃO		TOTAL		
1	1	Solução de antivírus com licenciamento perpétuo, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1	12.784	19.284		
				SJMG	3.500			
				UFT	3.000			
	2	Solução de antivírus com licenciamento perpétuo, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1	2.472	3.122		
				SJMG	450			
				UFT	200			
	3	Serviço de suporte técnico especializado	Meses	TRF1	12	36		
				SJMG	12			
				UFT	12			
	4	Treinamento	Alunos	TRF1	10	26		
				SJMG	6			
				UFT	10			
VALOR TOTAL DO GRUPO 1								
2	5	Solução de antivírus com licenciamento por meio de subscrição, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1	12.784	19.284		
				SJMG	3.500			
				UFT	3.000			
	6	Solução de antivírus com licenciamento por meio de subscrição, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses	Licença	TRF1	2.472	3.122		
				SJMG	450			
				UFT	200			
	7	Serviço de suporte técnico especializado	Meses	TRF1	12	36		
				SJMG	12			

				UFT	12			
	8	Treinamento	Alunos	TRF1	10	26		
				SJMG	6			
				UFT	10			
VALOR TOTAL DO GRUPO 2								

1. Prazo de entrega do objeto:.....(observar os prazos definidos no Termo de Referência);
2. Prazo de validade da proposta: ..... (observar prazo mínimo disposto no Edital).
3. Para fins de contratação, faturamento e pagamento de valor proposto constante do sistema Comprasnet considerar-se somente as duas primeiras casas após a vírgula, sem arredondamento.

DADOS DO REPRESENTANTE LEGAL:

Nome:

Cargo e Função na Empresa:

Brasília-DF, ____ de _____ de 20____.

_____
Razão Social da Empresa
Representante Legal
Função

Documento assinado eletronicamente por **Luiz Alberto Lima da Costa**, **Diretor(a) de Divisão**, em 08/08/2022, às 14:16 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Paulo de Tarso de Almada Santos**, **Analista Judiciário**, em 08/08/2022, às 14:44 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Rodrigo Alves Migueleti**, **Analista Judiciário**, em 08/08/2022, às 16:05 (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 **16275944** e o código CRC **3AD5DC38**.