PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO

ESTUDO TÉCNICO PRELIMINAR - ETP COMPLETO 0134303

(para contratação de serviços e/ou aquisição de bens permanentes e de consumo por licitação)

Guia de suporte ao preenchimento do ETP: 15238786

ID (PAC):

Não se aplica, pois a contratação não foi incluída no PAC-22.

A. Descrição sucinta do objeto

Contratação, por meio do sistema de Registro de Preços, de soluções de antivírus, incluindo serviços de suporte especializado e treinamento, para atender às necessidade da Justiça Federal da 6ª Região, de acordo com as especificações, condições e observações constantes deste Termo e de seus anexos.

B. Justificativa expressa para a contratação

A contratação é necessária para/porque *(expor a finalidade e os motivos da necessidade da contratação)*

B.1) O Tribunal Regional Federal da 6ª Região e as Subseções Judiciárias que compõem a Justiça Federal da Sexta 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.

B.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 Sexta Região, uma vez que não possuem mecanismos centralizados de gerência e impossibilitam a automação de execução das tarefas de instalação, configuração e atualização do antivírus

B.3. Grande parte das informações produzidas ou custodiadas na Justiça Federal da Sexta 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.

B.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 Sexta Região (TRF6) e Subseções Judiciárias da Justiça Federal da Sexta Região (JF6).

B.5. A segurança da informação é uma vertente cada vez mais necessária na composição da gestão de companhias e órgãos públicos, pois existe uma grande necessidade de proteção dos ativos organizacionais, além da crescente complexidade dos sistemas de negócio dos prestadores. 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.

B.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*.

B.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.

B.8. Para proteção do cidadão é necessário que os órgãos públicos investam cada vez mais em mecanismos mais robustos de proteção cibernética, dentre os quais 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.

B.9. As situações supracitadas demandam uma atenção especial ao monitoramento e proteção das estações de trabalho e dos equipamentos servidores da organização, razão pela qual é essencial a aquisição de uma ferramenta moderna com o objetivo de evitar pontos de vulnerabilidades na rede e possibilitar a geração de relatórios ou consultas para prover informações úteis ao gerenciamento do parque, de forma a fundamentar a adoção de ações preventivas e reativas.

B.10. Outro ponto de fundamental importância é que tal ferramenta seja dotada de uma gerência centralizada, de forma que seja possível conduzir a administração de todo o parque *antimalware* e garantir que as políticas e atualizações ocorram de forma imediata a todos os nós da rede protegida, assim como tornar a logística de instalação simplificada.

B.11. A contratação visa, ainda, os seguintes Benefícios Diretos e Indiretos:

B.11.1. Mitigar o risco de infestação das estações de trabalho e equipamentos servidores por ameaças virtuais.

B.11.2. Manter o controle das estações de trabalho com antivírus atualizado.

B.11.3. Aumentar a taxa de satisfação dos clientes internos e externos da JF6 com os serviços de TI.

B.11.4. Melhoria de nivelamento nos portes de tecnologia, capacitação e automação da 6ª Região.

B.11.5. Atualização tecnológica, de forma a proporcionar maior eficiência em relação aos trabalhos essenciais no âmbito da 6ª Região.

B.11.6. Maior rapidez na detecção de vírus e de ameaças virtuais.

B.11.7. 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.

B.11.8. Avisos e atualizações automáticas dos programas usados no JF6.

B.11.9. Controle de sites suspeitos, para evitar que sejam acessados e infectem o sistema da empresa.

B.11.10. 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.

B.11.11. Auxílio de suporte técnico, incluindo suporte on-site em eventuais problemas ou dúvidas que possam aparecer durante o uso do software.

B.11.12. Reestabelecimento da proteção das estações de trabalhos e equipamentos servidores, proporcionando maior segurança para a execução dos trabalhos essenciais no âmbito da 6ª Região.

A não contratação implicará *(expor as consequências advindas da não contratação)*

A manutenção da exposição da rede do TRF6 e das Subseções Judiciárias aos agentes maliciosos como vírus, *spywares*, *malwares*, entre outros.

C. Alinhamento da demanda com diretrizes e metas institucionais

- Resolução CNJ nº 370, de 28 de janeiro de 2021 - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CJF nº 685, de 15 de dezembro de 2020 - Plano Estratégico de Tecnologia da Informação da Justiça Federal

Macrodesafio: Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

Objetivos Estratégicos da Justiça Federal:

1) Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal

Indicadores	Metas
1 - Índice de satisfação dos clientes internos com os serviços de TI.	1 - Atingir, até 2025, 85% de satisfação dos clientes internos de TI.
2 - Índice de satisfação dos clientes externos com os serviços de TI.	2 - Atingir, até 2026, 80% de satisfação dos clientes externos de TI.

D. Proposta de solução

D.1. Alternativas de solução disponíveis no mercado

TABELA RESUMO

ID	SOLUÇÕES	ITENS	DESCRIÇÃO	QUANTIDADES TRF6	CUSTO UNITÁRIO	CONTRATAÇÕES SIMILARES ENCONTRADAS	FORNECEDORES AVALIADOS	ATENDE?
1	Aquisição de licença perpetua, com garantia técnica, atualização e suporte especializado pelo período de 60 (sessenta) meses, bem como serviços de desinstalação e treinamento.	1	Solução de antivírus (licença perpétua), para estações de trabalho com garantia e atualização das licenças, pelo período de 60 meses	3.500 Licenças	R$ 211,46	1 Contratações similares utilizadas. Ata de Registro de Preços nº 01/2022 - TSE (SEI TRF1 - 16125645)	4 Propostas Comerciais • QUALITEK (SEI TRF1 - 16129805) • SEPROL (SEI TRF1 - 16129811) • AX4B (SEI TRF1 - 16129818) • DFTI (SEI TRF1 - 16129829)	**SIM**
		2	Solução de antivírus (licença perpétua) para equipamentos servidores com garantia e atualização, pelo período de 60 meses	450 Licenças	R$ 227,96			
		3	Suporte especializado	12 Meses	R$ 11.900,00			
		4	Treinamento	6 Alunos	R$ 1.716,56			
2	Contratação de licença de uso (subscrição) com garantia técnica, atualização e suporte especializado pelo período de 60 (sessenta) meses, bem como serviços de desinstalação e treinamento.	1	Solução de antivírus (serviço de subscrição) para estação de trabalho com garantia técnica e atualização pelo período de 60 meses	3.500 Licenças	R$ 211,46	1 Contratações similares utilizadas. Ata de Registro de Preços nº 01/2022 - TSE (SEI TRF1 - 16125645)	4 Propostas Comerciais • QUALITEK (SEI TRF1 - 16129805) • SEPROL (SEI TRF1 - 16129811) • AX4B (SEI TRF1 - 16129818) • DFTI (SEI TRF1 - 16129829)	**SIM**
		2	Solução de antivírus (serviço de subscrição) para equipamentos servidores com garantia técnica e atualização pelo período de 60 meses	450 Licenças	R$ 227,96			
		3	Suporte especializado	12 Meses	R$ 11.900,00			
		4	Treinamento	6 Alunos	R$ 1.716,56			
3	Adoção de software livre com contratação de serviços de suporte especializado, treinamento e desinstalação.	1	Solução de antivírus para estação de trabalho	3.500 Licenças	-	-	3 Soluções de antivírus livre avaliadas.	**NÃO**
		2	Solução de antivírus para equipamentos servidores	450 Licenças	-	-		
		3	Suporte especializado	12 Meses	-	-		
		4	Treinamento	6 Alunos	-	-		

4	Upgrade das licenças atuais	-	-	-	-	-	-	**NÃO**

SOLUÇÃO 01 - SOLUÇÃO SIMILAR ADOTADA EM OUTRO ÓRGÃOS

ÓRGÃO	**ITEM**	**DESCRIÇÃO**	**UNIDADE DE MEDIDA**	**QUANT**	**VALOR UNITÁRIO**	**INFORMAÇÃO RELEVANTE** (Comparação entre as especificações técnicas do TRF6 em relação a prevista no Edital do órgão similar)	**ATENDE?**
	30	DVD - licença antivírus para computadores, ou notebooks, original, licenciado	Unidade	215	R$ 79,00	• Relatório Banco de Preços (SEI TRF1 - 14543977) • Preço (Compras Governamentais) 1 - Pág 2. • Edital - (SEI TRF6 - 14543845) • Data do Pregão: 14/06/2021 • Fornecedor vencedor: BRINFOR SOLUCOES EM TILTDA • Solução ofertada foi do fabricante BITDEFENDER modelo advanced. • Link da solução ofertada: Bitdefender GravityZone Advanced Business Security • Não tem informação de prazo de garantia da solução. • **O valor do item não pode ser utilizado devido a data de homologação do pregão ocorrer a mais de 01 ano.** • **Tecnicamente a solução não atende aos requisitos do tribunal no tocante a necessidade da soluções e sobretudo dos agentes serem de um mesmo fabricante**.	**NÃO**

PREFEITURA MUNICIPAL DE CRISTAIS Pregão 20/2021 UASG: 984403	31	DVD - licença antivírus para servidor dell powered t- 310, para windows server 2016 64bits r2, original, licenciado.	Unidade	1	R$ 79,00	• Relatório Banco de Preços (SEI TRF1 - 14543977) • Preço (Compras Governamentais) 2 - Pág 2. • Edital - (SEI TRF6 - 14543845) • Data do Pregão: 14/06/2021 • Fornecedor vencedor: BRINFOR SOLUCOES EM TILTDA • Solução ofertada foi do fabricante BITDEFENDER modelo advanced. • Link da solução ofertada: Bitdefender GravityZone Advanced Business Security • Não tem informação de prazo de garantia da solução. • **O valor do item não pode ser utilizado devido a data de homologação do pregão ocorrer a mais de 01 ano.** • **Tecnicamente a solução não atende aos requisitos do tribunal no tocante a necessidade da soluções e sobretudo dos agentes serem de um mesmo fabricante**.	**NÃO**

INST.FED.DE EDUC.CIENC. E TEC. DO MARANHÃO - IFMA Dispensa 3/2021 UASG:154855	1	Solução de Software Antivírus (Kaspersky Endpoint Security) utilizada em Servidores , Estações Linux e Windows do Instituto Federal de Educação, Ciência e Tecnologia do Maranhão Campus Pedreiras.	Licença	150	R$ 59,70	• Relatório Banco de Preços (SEI TRF1 - 14543977) • Preço (Compras Governamentais) 4 - Pág 3. • Data da Compra: 01/05/2021 • Fornecedor vencedor: VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA EIRELI • Solução ofertada: Kaspersk Software Antivírus (Kaspersky Endpoint Security) • Prazo de vigência da garantia técnica: atualização e suporte da solução de antivírus por 12 meses. • Pagamento: por ser dispensa de licitação não há Edital para consulta. • **O valor do item não pode ser utilizado devido a data de homologação do pregão ocorrer a mais de 01 ano.** • **Embora o fabricante possua solução que atenda tecnicamente aos requisitos do tribunal, o objeto do fornecimento ao IFMA não contempla todos os módulos requeridos pelo tribunal**.	**NÃO**

TJRN - TRIBUNAL DE JUSTIÇA DO ESTADO DO RN Pregão 02/2021 UASG: 925869	1	Licença de uso perpétua de solução antivírus corporativa, com atualização e suporte.	Licenças	5.500	R$ 75,99	• Termo de Homologações dos PE (SEI TRF1 16129834). • Edital - (SEI TRF1 - 14543858 e 14609439) • Data de homologação: 04/02/2021 • Fornecedor vencedor: QUALITEK TECNOLOGIA LTDA • Solução ofertada: KASPERSKY • Prazo de vigência da garantia técnica: Para garantir a entrega, instalação, suporte, atualizações e transferência de conhecimento da solução, o contrato deve ter validade de 48 meses. • Pagamento: 1 parcela única após recebimento definitivo. • **O valor do item não pode ser utilizado, embora o fabricante possua solução que atenda tecnicamente aos requisitos do tribunal, o objeto do fornecimento ao TJRN não contempla todos os módulos requeridos pelo tribunal, tais quais como o *sandbox* e solução de detecção e resposta de incidentes**.	**NÃO**

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA Pregão 03/2021 UASG: 926363	1	Contratação de serviços de renovação e expansão de licenças de software antivírus BitDefender versão Advanced Business Security, suporte, garantia e atualização por 36 (trinta e seis) meses.	Licenças	230	R$ 108,00	• Relatório Painel de Preços (SEI TRF1 - 14543964) - Resultado 4 - Pág. 4. • Edital - (SEI TRF1 - 14543894) • Data de homologação: 16/03/2021 • Fornecedor vencedor: CERTA INFORMATICA LTDA • Solução ofertada: BitDefender versão Advanced Business Security • Prazo de vigência da garantia técnica: suporte, garantia e atualização por 36 (trinta e seis) meses. • Pagamento: parcela única após recebimento definitivo. • **O valor do item não pode ser utilizado devido a data de homologação do pregão ocorrer a mais de 01 ano.** • **Tecnicamente a solução não atende aos requisitos do tribunal no tocante a necessidade da soluções e sobretudo dos agentes serem de um mesmo fabricante**.	**NÃO**

DEPARTAMENTO ESTADUAL DE TRÂNSITO - RO Pregão 49/2018 UASG: 926002	1	Aquisição de renovação da Garantia e Suporte de 1800 (Hum mil e Oitocentas) Licenças do Software, Antivírus Corporativo Kaspersky Endpoint Security for Business Select, de acordo com a justificativa, quantidades e especificações técnicas constantes no Anexo I Termo de Referência	Licenças	1.800	R$ 57,50	• Relatório Painel de Preços (SEI TRF1 - 14543964) - Resultado 1 - Pág. 1. • Edital - (SEI TRF1 - 14543904) • Data de homologação: 21/08/2020 • Fornecedor vencedor: RL2 SERVICOS DE INFORMATICA LTDA • Solução ofertada: Kaspersky Endpoint Security for Business Select • Prazo de vigência da garantia técnica: 24 (vinte e quatro) meses. • Pagamento: parcela única. • **O valor do item não pode ser utilizado devido a data de homologação do pregão ocorrer a mais de 01 ano.,** • **embora o fabricante possua solução que atenda tecnicamente aos requisitos do tribunal, o objeto do fornecimento ao DETRAN-RO não contempla todos os módulos requeridos pelo tribunal. tais quais como o *sandbox* e solução de detecção e resposta de incidentes**.	**NÃO**

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO CNMP Pregão 9/2021 UASG: 590001	1	Contratação de empresa autorizada pelo fabricante para renovação e fornecimento do período de garantia de atualização de versão e suporte técnico especializado, pelo período de 12 meses.	Licenças	600	R$ 122,75	• Relatório Banco de Preços (SEI TRF1 - 14543977) • Preço (Compras Governamentais) 3 - Pág 3. • Edital - (SEI TRF1 - 14543916) • Data de homologação: 07/06/2021 • Fornecedor vencedor: DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA • Solução ofertada: subscrição Trend Micro – Apex One e Apex - Central em nuvem (SaaS) • Prazo de vigência da garantia técnica: 12 meses • Pagamento: O pagamento do serviço de garantia de atualização e suporte técnico dar-se-á mensalmente, devendo o valor total ser dividido em 12 (doze) parcelas iguais. • **O valor do item não pode ser utilizado devido a data de homologação do pregão ocorrer a mais de 01 ano.** • **Embora o fabricante possua solução que atenda tecnicamente aos requisitos do tribunal, o objeto do fornecimento ao CNMP não contempla todos os módulos requeridos pelo tribunal**.	**NÃO**
TRIBUNAL	1	Licenças de software de segurança (para estações de trabalho e servidores) + console de gerenciamento/ garantia / atualizações/ suporte técnico / manutenção preventiva e corretiva por 48 meses.	Licenças	82.809	R$ 125,60	• Valores conforme registrados na Ata de Registro de Preços nº 05/2021 - TRT13 (SEI TRF1 - 16125819) • Edital - (SEI TRF1 - 14543934 e 14609792) • Validade: 09/08/2022 • Fornecedor	
	2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento/Garantia/Atualização/Suporte Técnico/Manutenção	Licenças	5.136	R$ 125,60		
	3	Implantação e configuração da solução + Repasse de conhecimento hands-on	Serviço	28	R$ 16.000,00		

REGIONAL DO TRABALHO 13ª REGIÃO Pregão 11/2021 ARP 05/2021	4	Treinamento EAD	Alunos	189	R$ 2.600,00	vencedor: ISH • Solução ofertada: Kaspersky EDR OPTIMUM • Prazo de vigência da garantia técnica: 48 meses • Pagamento: parcela única. • **O valor do item não pode ser utilizado devido a vigência inferior a 60 meses**.	**NÃO**

SOLUÇÃO 02 - SOLUÇÃO SIMILAR ADOTADA EM OUTROS ÓRGÃOS							
ÓRGÃO	**ITEM**	**DESCRIÇÃO**	**UNIDADE DE MEDIDA**	**QUANT.**	**VALOR UNITÁRIO**	**INFORMAÇÃO RELEVANTE** (Comparação entre as especificações técnicas do TRF6 em relação a prevista no Edital do órgão similar)	**ATENDE?**
INST.FED.DE EDUC.CIENC.E TEC.DO SUL DE MG - MEC Pregão 03/2021 USAG 158137	1	Subscrição de licenças de software antivírus	Licenças	4.410	R$ 22,50	• Termo de Homologações dos PE (SEI TRF1 - 16129834). • Edital - (SEI TRF1 - 14544002) • Data de homologação: 06/04/2021 • Fornecedor vencedor: S G SOLUCOES TECNOLOGICAS LTDA • Solução ofertada: F-SECURE PROTECTION SERVICE FOR BUSINESS • Prazo de vigência da garantia técnica: 12 meses. • Prazo de vigência da garantia técnica: A vigência da subscrição da licença do software antivírus deverá ser de 12 (doze) meses, contados da data de emissão do termo de aceitação correspondente aos processos de fornecimento, instalação, ativação e testes. • Pagamento: parcela única. • **O valor do item não pode ser utilizado para fins de estimativa do valor da contratação, pois a garantia técnica possui vigência inferior a 60 meses**.	**NÃO**

INSTITUTO NACIONAL DE TRAUMATO-ORTOPEDIA - MS Pregão 09/2021 USAG 250057	3	Aquisição de ferramentas de segurança de rede (antispam, antivírus e outros) do Instituto Nacional de Traumatologia e Ortopedia Jamil Haddad – INTO	Licenças	1500	R$ 92,00	• Termo de Homologações dos PE (SEI TRF1 - 16129834). • Edital - (SEI TRF1 - 14544019) • Data de homologação: 03/03/2021 • Fornecedor vencedor: PTLS SERVICOS DE TECNOLOGIA E ASSESSORIA TECNICA LTDA • Solução ofertada: Fabricante CISCO -P/N: ESA-ESP-LIC= / ESA-ESP-3Y-S4 • Prazo de vigência da garantia técnica: incluindo serviços de manutenção, upgrade, updates, suporte técnico e garantia pelo prazo de 36 (trinta e seis) meses. • Pagamento: parcela única. • **Nosso objeto não é uma Appliance, no caso o pregão foi analisado e considerado apenas para apresentação do modelo de contratação por cessão de uso, mesmo modelo que está sendo considerado neste cenário.** • **O valor do item não pode ser utilizado para fins de estimativa do valor da contratação, pois a garantia técnica possui vigência inferior a 60 meses**.	**NÃO**
INST.FED.EDUC.CIENC.E TEC.SERTÃO PERNAMBUCANO - MEC Pregão 02/2021 UASG 158149	1	Contratação de empresa especializada para prestação de serviço de fornecimento de licenças para solução de antivírus corporativo para o IF Sertão-PE.	Licenças	1.908	R$ 71,50	• Termo de Homologações dos PE (SEI TRF1 - 16129834). • Edital - (SEI TRF1 - 14544063) • Data de homologação: 09/02/2021 • Fornecedor vencedor: UNITEC SOLUCOES EM TI LTDA • Solução ofertada: ESET Endpoint Protection Advanced • Prazo de vigência da garantia técnica: Garantia e atualização por 36 (trinta e seis) meses. • Pagamento: parcela única • **O valor do item não pode ser utilizado para fins de estimativa do valor da contratação, pois a garantia técnica possui vigência inferior a 60 meses**.	**NÃO**

UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ - MEC Pregão 04/2021 UASG 158718	1	Renovação de licença de software antivírus da fabricante Kaspersky, com suporte e garantia para 36 (trinta e seis) meses.	Licenças	1.000	R$ 81,70	• Termo de Homologações dos PE (SEI TRF1 - 16129834). • Edital - (SEI TRF11 - 14544075) • Data de homologação: 29/04/2021 • Fornecedor vencedor: VTECH COMERCIO, SERVICOS E EQUIPAMENTOS DE INFORMATICA EIRELI • Solução ofertada: Kaspersky • Prazo de vigência da garantia técnica: 36 meses. • Pagamento: parcela única. • **Trata-se de renovação de licença de software de antivírus, não sendo possível a utilização.** • **O valor do item não pode ser utilizado para fins de estimativa do valor da contratação, pois a garantia técnica possui vigência inferior a 60 meses**.	**NÃO**
CONSELHO REGIONAL DE MEDICINA ES.S.CATARINA - CRMSC Pregão 06/2021 UASG 389180	1	Aquisição de solução de antivírus corporativo por 12 (doze) meses, renováveis até o prazo legal de 48 meses, incluindo garantia de atualização contínua, serviços de treinamento, instalação, configuração, manutenção corretiva e preventiva e suporte técnico especializado para proteção dos equipamentos do ambiente de TIC do CRM-SC.	Licenças	150	R$ 88,00	• Termo de Homologações dos PE (SEI TRF1 - 16129834). • Edital - (SEI TRF1 - 14544086) • Data de homologação: 28/04/2021 • Fornecedor vencedor: ISTI INFORMATICA & SERVICOS LTDA • Solução ofertada: BITDEFENDER • Prazo de vigência da garantia técnica: 12 meses renováveis por até 48 meses. • Pagamento: 1 parcela única anual a ser paga até 30 dias úteis após recebimento definitivo. • **O valor do item não pode ser utilizado para fins de estimativa do valor da contratação, pois a garantia técnica possui vigência inferior a 60 meses**.	**NÃO**
INDUSTRIAS NUCLEARES DO BRASIL S/A - MINISTÉRIO DE MINAS E ENERGIA Pregão 01002/2021 UASG 113206	1	Cessão temporária de direitos sobre programas de computador locação de software - INBOUND ESSENTIALS BUNDLE (AS+AV+OF) 3YR LIC, 1K-1999 USERS	Licenças	1.500	R$ 125,7	• Termo de Homologações dos PE (SEI TRF1 - 16129834). • Edital - (SEI TRF1 - 14544097) • Data de homologação: 11/02/2021 • Fornecedor vencedor: YSSY SOLUCOES S.A. • Solução ofertada: Cisco IronPort email security appliance • Prazo de vigência da garantia técnica: As licenças deverão ser válidas por 36 (trinta e seis) meses. • Pagamento: parcela única • **Nosso objeto não é uma Appliance, no caso o pregão foi analisado e considerado apenas para apresentação do modelo**	**NÃO**

	2	Serviços de instalação, transição e configuração / parametrização de software	Und.	1	R$ 17.450,00	**de contratação por cessão de uso, mesmo modelo que está sendo considerado neste cenário.** • **O valor do item não pode ser utilizado para fins de estimativa do valor da contratação, pois a garantia técnica possui vigência inferior a 60 meses**.	
FUNDAÇÃO NACIONAL DE ARTES - FUNARTE Pregão 8/2020 UASG 403201	1	Solução de antispam e segurança de e-mail com licença, suporte, garantia, implantação e subscrição no regime 24*7, válido pelo período de 12 (doze) meses.	UND.	2	R$ 135.693,88	• Termo de Homologações dos PE (SEI TRF1 - 16129834). • Edital - (SEI TRF1 - 14544126) • Data de homologação: 14/01/2021 • Fornecedor vencedor: ZIVA TECNOLOGIA E SOLUCOES LTDA. • Prazo de vigência da garantia técnica: 12 meses e 36 meses • Pagamento: parcela única • **Nosso objeto não é antispam, mas sim antivírus, no caso o pregão foi analisado e considerado apenas para apresentação do modelo de contratação por cessão de uso, mesmo modelo que está sendo considerado neste cenário.** • **O valor do item não pode ser utilizado para fins de estimativa do valor da contratação, pois a garantia técnica possui vigência inferior a 60 meses**.	**NÃO**
	2	Licença, suporte, garantia, implantação e subscrição para solução de antispam e segurança de e-mail no regime 24*7, válido pelo período de 36 (trinta e seis) meses.	UND.	2	R$ 165.520,04		
	3	Licença, suporte, garantia, implantação e subscrição de expansão da solução forticlient ems para 500 clientes no regime 24*7 pelo período de 12 (doze) meses.	UND.	2	R$ 41.304,69		
	4	Licença, suporte, garantia, implantação e subscrição de expansão da solução forticlient ems para 500 clientes no regime 24*7 pelo período de 36 (trinta e seis) meses	UND.	2	R$ 132.919,71		
	5	Licença, suporte, garantia, implantação e subscrição de expansão da solução forticlient ems em mais 100 (cem) clientes no regime 24*7 pelo período de 36 (trinta e seis) meses.	UND.	6	R$ 39.425,84		

CONSELHO REG. DE ENGENHARIA E AGRONOMIA DO PR - CREA-PR Pregão 26/2020 UASG 389088	1	Renovação (atualização) das licenças InterScan Messaging Security Virtual Appliance Academic do fabricante Trend Micro PartNumber IMRA0107, vigência de 36 meses	UND.	501 licenças	R$ 179.799,00 Valor Total	• Termo de Homologações dos PE (SEI TRF1 - 16129834). • Edital - (SEI TRF1 - 14544130) • Data de homologação: 05/01/2021 • Fornecedor vencedor: PBI INFORMATICA LTDA • Solução ofertada: Trend Micro • Prazo de vigência da garantia técnica: 36 (trinta e seis) meses. • Pagamento: das licenças em parcela única. • **Nosso objeto não é *antispam*, mas sim antivírus, no caso o pregão foi analisado e considerado apenas para apresentação do modelo de contratação por cessão de uso, mesmo modelo que está sendo considerado neste cenário.** • **O valor do item não pode ser utilizado para fins de estimativa do valor da contratação, pois a garantia técnica possui vigência inferior a 60 meses**.	**NÃO**
	2	Renovação (atualização) das licenças Trend Micro Enterprise Security for Endpoints (Advanced) Academic do fabricante Trend Micro, PartNumber ENRA0206, vigência de 36 meses	UND.	501 licenças			
	3	Prestação de serviços de suporte técnico	Horas	Até 100 horas			
TSE - TRIBUNAL SUPERIOR ELEITORAL Pregão 84/2021 UASG: 70001	1	Solução de segurança de EndPoint (desktops), com EDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. Marca: TRENDMICRO Modelos: Trend Micro Smart Protection for Endpoints + EDR/XDR: Endpoint and Server + Deep Discovery Analyzer	UND.	35.906	R$ 197,00	• Valores conforme registrados na Ata de Registro de Preços nº 01/2022 - TSE (SEI TRF1 - 16125645). • Vigência da ARP 01/2022: 10/01/2023 • Solução ofertada: TRENDMICRO • Solução de Segurança de EndPoint (desktops), com XDR e *Sandbox*. • Manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. • Objeto atende ao desejado pela JF6, inclusive contém os serviços de XDR e *Sandbox* que é solicitado nas especificações. • Valor utilizado para composição dos prazos.	**SIM**
	2	Solução de Segurança de EndPoint (desktops), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. Marca: TRENDMICRO Modelos: Trend Micro Smart Protection for Endpoints + Deep Security System + XDR: Endpoint and Server + Deep Discovery Analyzer	UND.	21.077	R$ 197,00		

	3	Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. Marca: TRENDMICRO Modelos: Trend Micro Smart Protection for Endpoints + Deep Security System + XDR: Endpoint and Server + Deep Discovery Analyzer	UND.	8.360	R$ 230,00		
	4	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única)	UND.	28	R$ 3.000,00		
	5	Transferência de conhecimento (parcela única).	UND.	4	R$ 8.000,00		

D.2. Estimativa de preços das alternativas de solução

PROPOSTAS COMERCIAIS - SOLUÇÕES 1 e 2

Destaca-se que as soluções 1 e 2 são para o mesmo objeto e o que muda e o tipo de licenciamento (licença perpétua ou subscrição) e considerando que será homologado apenas o grupo que restar com menor valor, foi realizado uma mescla da estimativa e utilizado o mesmo valor para ambos os grupos das propostas comerciais recebidas.

FORNECEDOR	ID	DESCRIÇÃO	UNIDADE	VALOR UNITÁRIO	INFORMAÇÃO RELEVANTE	ATENDE?
QUALITEK (SEI TRF1 - 16129805)	1	Solução de antivírus, para estações de trabalho	Licença	R$ 495,00	• Data da proposta: 08/06/2022 • Solução ofertada: Kaspersky Endpoint Detection and Response Optimum (Base Plus) License + Kaspersky Sandbox	**SIM**
	2	Solução de antivírus, para equipamentos servidores	Licença	R$ 900,00		
	3	Suporte especializado	Meses	R$ 30.000,00		
	4	Treinamento	Alunos	R$ 6.000,00		
SEPROL (SEI TRF1 - 16129811)	1	Solução de antivírus, para estações de trabalho	Licença	R$ 640,00	• Data da proposta: 20/07/2022 • Solução ofertada: Harmony Endpoint Protection	**SIM**
	2	Solução de antivírus, para equipamentos servidores	Licença	R$ 640,00		
	3	Suporte especializado	Meses	R$ 15.558,35		
	4	Treinamento	Alunos	R$ 1.716,60		
AX4B (SEI TRF1 - 16129818)	1	Solução de antivírus, para estações de trabalho	Licença	R$ 225,92	• Data da proposta: 12/07/2022 • Solução ofertada: ESET PROTECT Enterprise	**SIM**
	2	Solução de antivírus, para equipamentos servidores	Licença	R$ 225,92		
	3	Suporte especializado	Meses	R$ 11.900,00		
	4	Treinamento	Alunos	R$ 12.000,00		
DFTI (SEI TRF1 - 16129829)	1	Solução de antivírus, para estações de trabalho	Licença	R$ 305,00	• Data da proposta: 15/07/2022 • Solução ofertada: GravityZone Business Security Enterprise	**SIM**
	2	Solução de antivírus, para equipamentos servidores	Licença	R$ 305,00		
	3	Suporte especializado	Meses	R$ 17.500,00		
	4	Treinamento	Alunos	R$ 2.400,00		

D.3. Razões da escolha da melhor solução (justificar técnica e economicamente o que o levou a escolher a solução)

DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

D.3.1. ID da Solução: 01 ou 02

D.3.2. Descrição da Solução:

D.3.2.1.1. Deverá ser adotado o Sistema de Registro de Preços, conforme estabelece o Decreto 7.892, de 23 de janeiro de 2013, pelos seguintes aspectos:

- Dentre o levantamento apresentado, o mais viável será aquele que atender aos princípios da viabilidade técnica respeitado a economicidade, desta maneira a equipe de planejamento recomenda o **Registro de Preços, com base nos inciso IV -** quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.
- 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.

D.3.2.1.2. Desta maneira será realizado Registro de Preços para as seguintes alternativas:

- Solução de antivírus, com licenciamento perpétuo.
- Solução de antivírus com licenciamento por meio de subscrição.

D.3.3. Não há diferenciação técnicas entre as soluções 01 e 02, sendo a única mudança a forma de comercialização. A solução 01 visa adquirir licenças perpétuas e a solução 02 visa a contratação de subscrição do produto. Considerando a velocidade que os ataques evoluem e a necessidade de manter uma proteção atualizada para o nosso parque computacional, após o vencimento da garantia da solução, a estagnação da base de dados de ameaças apresentará falhas na proteção cibernética. Adiciona-se ao fato das mudanças constantes do mercado de Cibersegurança que em alguns casos impossibilita a expansão da garantia e atualização do produto, como exemplo o contrato TRF1 n. 66/2018 onde o fabricante informa que a licença atual não é passível de upgrade conforme documento (SEI TRF1 - 15852837), tornando as licenças adquiridas pelo TRF1 obsoletas e que não agregam proteção ao parque. Por tal razão, considera-se que a solução por licenciamento perpétuo e por subscrição com garantia de 60 meses cada são equivalentes e competitivas entre si.

D.3.3.1. Com relação aos grandes fornecedores do mercado, observa-se que nos últimos anos surgiram ferramentas que só oferecem o produto no formato subscrição. Por exemplo: CheckPoint, CrowdStrike, Sophos, etc.

D.3.3.2. Considerando que a ampliação da competitividade do certame pode incorrer em vantagem econômica para este Tribunal, dificilmente vislumbrado na fase de planejamento, este certame ocorrerá dividido em dois lotes, um contemplando licenciamento perpétuo e outro considerando subscrição. Este Tribunal irá adquirir somente o lote com o melhor preço.

D.3.4. Considerando que a ampliação da competitividade do certame pode incorrer em vantagem econômica para este Tribunal, dificilmente vislumbrado na fase de planejamento, este certame ocorrerá dividido em dois lotes, um contemplando licenciamento perpétuo e outro considerando subscrição. Este Tribunal irá adquirir somente o lote com o melhor preço.

D.3.4. O Tribunal Regional Federal da 6ª Região e as Subseções Judiciárias que compõem a Justiça Federal da Sexta 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.

D.3.5. Considerando o quantitativo de licenças, 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 Sexta Região, visto que não possuem mecanismo centralizado de gerência e impossibilitam automação de execução das tarefas de instalação, configuração e atualização do antivírus

D.3.6. Grande parte das informações produzidas ou custodiadas na Justiça Federal da Sexta 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.

D.3.7. Para prover segurança aos usuários da JF6 foram levantados 5 cenários, sendo que apenas os cenários 1 e 2 atendem a todos os requisitos de negócio/técnicos, embora a solução 02 apresenta desvantagem econômica para a JF6, foram encontras mais fornecedores ofertando o produto, por este motivo optou-se por aumentar a competitividade e após a homologação do certame será adquirido somente o lote que apresentar melhor vantagem econômica.

D.3.7.1.Destaca-se que as informações em relação a desvantagem econômica da solução nº 2 apontada no subitem 8.7 consta da versão anterior do ETP do TRF1 (SEI TRF1 - 15013078).

D.3.8. Bens e Serviços que Compõem a Solução:

GRUPOS	ITENS	DESCRIÇÃO	QUANTIDADES	UNIDADE DE MEDIDA	CUSTO UNITÁRIO	CUSTO TOTAL
1	1	Solução de antivírus com licenciamento perpétuo para estações de trabalho, com garantia e atualização da solução pelo período de 60 meses	3.500	Licenças	R$ 211,46	R$ 740.110,00
	2	Solução de antivírus com licenciamento perpétuo para equipamentos, servidores, com garantia e atualização da solução pelo período de 60 meses	450	Licenças	R$ 227,96	R$ 102.582,00
	3	Serviço de Suporte Técnico Especializado	12	Meses	R$ 11.900,00	R$ 142.800,00
	4	Treinamento	6	Alunos	R$ 1.716,56	R$ 10.299,36
VALOR TOTAL GRUPO 1						**R$ 995.791,36**

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	3.500	Licenças	R$ 211,46	R$ 740.110,00
	6	Solução de antivírus com licenciamento por meio de subscrição para equipamentos servidores, com garantia e atualização da solução pelo período de 60 meses	450	Licenças	R$ 227,96	R$ 102.582,00
	7	Serviço de Suporte Técnico Especializado	12	Meses	R$ 11.900,00	R$ 142.800,00
	8	Treinamento	6	Alunos	R$ 1.716,56	R$ 10.299,36
VALOR TOTAL GRUPO 2						**R$ 995.791,36**

D.3.9. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

D.3.9.1. Quanto a Solução 03 - Adoção de software livre - Destaca-se que o cenário 3 não atende aos requisitos técnicos e de negócio, uma vez que as soluções avaliadas não se mostram adequadas para ambientes corporativos, assim como não possuem ferramenta que possibilite "centralizar o gerenciamento promovendo o controle e monitoramento efetivo da solução em toda a JF6".

D.3.9.2. Quanto a Solução 04 - Upgrade das licenças atuais - Conforme informação disponível no site do fabricante SEI TRF1 - 15852837, as licenças atualmente utilizadas no TRF6 não possuem *upgrade* de versão, assim o cenário de upgrade de versão não atende aos requisitos de negócio desta administração.

D.3.9.3. Por tais razões, as soluções 03 e 04 são consideradas inviáveis.

D.4. Justificativas para o parcelamento ou não da solução

D.4.1. No presente caso a contratação de todos os itens de cada lote 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 JF6 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.

D.4.2. 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 JF6, 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. Ademais, também, justifica-se o não parcelamento do objeto no presente caso pelo aumento da eficiência administrativa por meio da otimização do gerenciamento do fornecedor.

D.4.3. Deste modo, o não parcelamento dos lotes 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.

D.4.1. Aplicação de cotas a microempresas (ME) e empresas de pequeno porte (EPP)(somente para bens de natureza divisível)

Não se aplica, em virtude da necessidade de aquisição dos itens em conjunto.

E. Requisitos da solução escolhida

E.1. Requisitos qualitativos e quantitativos (e análise das contratações anteriores)

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 6ª Região - JF6.

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 JF6, 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 da JF6;

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 JF6 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 JF6 no Active Directory: TRF6 > Subseções Judiciárias.

1.2.15. Deverá permitir visualização ou agrupamento dos agentes instalados e gerenciados de forma a refletir a estrutura hierárquica da JF6, na forma representada no Active Directory, observando a ordem: Tribunal Regional Federal da 6ª Região - TRF6 > Subseção Judiciária;

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 (TRF6/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 JF6;

1.2.21.2. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da JF6;

1.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da JF6 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 JF6 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 JF6;

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 JF6, observando a ordem: TRF6 > Subseção Judiciária;

1.4.6. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as 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/TRF6;

1.4.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção/TRF6, 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 JF6, 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 6ª Região - JF6;

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

2.1.4. A solução deverá ser fornecida pronta para utilização imediata da JF6, 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 do TRF6;

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 JF6 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 JF6 no Active Directory: TRF6 > Subseções Judiciárias

2.2.15. Deverá permitir visualização ou agrupamento dos agentes instalados e gerenciados de forma a refletir a estrutura hierárquica da JF6, na forma representada no Active Directory, observando a ordem: Tribunal Regional

Federal da 6ª Região - TRF6 > Subseção Judiciária;

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 JF6;

2.2.21.2. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da JF6;

2.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da JF6 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 JF6 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 JF6;

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 JF6, observando a ordem: TRF6 > Subseção Judiciária;

2.4.6. A instalação dos agentes deverá ser realizada de forma remota, abrangendo todas as 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/TRF6;

2.4.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção//TRF6, 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 JF6, 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 JF6.
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 TRF6, 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 TRF6.

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 6ª Região - JF6;

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 JF6, 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 do TRF6;

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 JF6 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 JF6 no Active Directory: TRF6 > Subseções Judiciárias.

5.2.15. Deverá permitir visualização ou agrupamento dos agentes instalados e gerenciados de forma a refletir a estrutura hierárquica da JF6, na forma representada no Active Directory, observando a ordem: Tribunal Regional Federal da 6ª Região - TRF6 > Subseção Judiciária;

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 (TRF6/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 JF6;

5.2.21.2. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da JF6;

5.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da JF6 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 JF6 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 JF6;

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 JF6, observando a ordem: TRF6 > Subseção Judiciária;

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/TRF6;

5.4.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção//TRF6, 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 JF6, 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 6ª Região - JF6;

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

6.1.4. A solução deverá ser fornecida pronta para utilização imediata da JF6, 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 do TRF6;

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 JF6 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 JF6 no Active Directory: TRF6 > Subseções Judiciárias

6.2.15. Deverá permitir visualização ou agrupamento dos agentes instalados e gerenciados de forma a refletir a estrutura hierárquica da JF6, na forma representada no Active Directory, observando a ordem: Tribunal Regional Federal da 6ª Região - TRF6 > Subseção Judiciária;

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 JF6;

6.2.21.2. Administradores locais, com acesso a funcionalidades específicas e em pontos de domínios específicos da estrutura hierárquica da JF6;

6.2.21.3. Visualização ou monitoramento, podendo abranger todo contexto da estrutura hierárquica da JF6 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 JF6 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 JF6;

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 JF6, observando a ordem: TRF6 > Subseção Judiciária;

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//TRF6;

6.4.10.2. Sumarização no formato gráfico ou tabular com agrupamento por localidade – Subseção//TRF6, 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 JF6, 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 TRF6, 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 TRF6.

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

E.2. Critérios de sustentabilidade

Os itens pretendidos são sustentáveis? Indicar a resposta expressamente para cada item (SIM ou NÃO).
*Em caso de resposta **afirmativa** para um ou mais itens: indicar os critérios de sustentabilidade adotados para cada item.*
*Em caso de resposta **negativa** para um ou mais itens: justificar o afastamento dos critérios de sustentabilidade para cada item.*

Não se aplica.

E.3. Critérios de acessibilidade

Não se aplica.

E.4. Demonstração de que o mercado atende aos requisitos mínimos

REQUISITOS	ID DO CENÁRIO	SIM	NÃO	NÃO SE APLICA
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	01	X		
	02	X		
	03		X	
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	01	X		
	02	X		
	03		X	
A Solução está disponível no Portal do Software Público Brasileiro?	01		X	
	02		X	
	03		X	
A Solução é um software livre ou software público?	01		X	
	02		X	
	03	X		
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	01			X
	02			X
	03			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	01			X
	02			X
	03			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq – Jus?	01			X
	02			X
	03			X

F. Descrição da solução como um todo

F.1. Resultados pretendidos com a solução escolhida

Pretende-se com a contratação:

- Mitigar o risco de infestação das estações de trabalho e equipamentos servidores por ameaças virtuais;
- Manter o controle das estações de trabalho com antivírus atualizado;
- Aumentar a taxa de satisfação dos clientes internos e externos da JF6 com os serviços de TI;
- Melhoria de nivelamento nos portes de tecnologia, capacitação e automação da 6ª Região;
- Atualização tecnológica, de forma a proporcionar maior eficiência em relação aos trabalhos essenciais no âmbito da 6ª Região;
- Maior rapidez na detecção de vírus e de ameaças virtuais;
- 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;
- Avisos e atualizações automáticas dos programas usados no JF6;
- Controle de sites suspeitos para evitar que sejam acessados e infectem os sistemas do TRF6;
- 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;
- Auxílio de suporte técnico, incluindo suporte on-site em eventuais problemas ou dúvidas que possam aparecer durante o uso do software;
- Restabelecimento da proteção das estações de trabalhos e equipamentos servidores, proporcionando maior segurança para a execução dos trabalhos essenciais no âmbito da 6ª Região.

F.2. Contratações correlatas e/ou interdependentes

Pregão Eletrônico nº 00024/2022 (SRP) do Tribunal Regional Federal da 1ª Região.

F.3. Adequações do ambiente do órgão impostas pela solução escolhida

Não se aplica.

F.4. Descrição integral da solução

Contratação de prestador especializado para o 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 6ª Região, de acordo com as especificações, condições e observações do Termo de Referência SEI TRF1 16421447.

G. Declaração de viabilidade

Com base nas informações levantadas ao longo deste estudo técnico, declaramos que a solução apresentada é viável de prosseguir e ser concretizada, pois é a que melhor atende os requisitos técnicos e funcionais pretendidos pela área demandante.

H. Nome e assinatura dos responsáveis pela elaboração e pela revisão, supervisão e controle de qualidade do ETP

Responsável pela elaboração: *(servidor da unidade requisitante)*
Heli Lopes Rios - Diretor da Subsecretaria de Infraestrutura - SUINF - Integrante Técnico
Cristiane de Figueiredo Gomes - Integrante Admnistrativo
Responsável pela revisão, supervisão e controle de qualidade: *(diretor)*
Daniel Santos Rodrigues - Diretor da Secretaria de Tecnologia da Informação - SECTI

Documento assinado eletronicamente por **Heli Lopes Rios**, **Diretor(a) de Subsecretaria**, em 05/12/2022, às 15:06, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Daniel Santos Rodrigues**, **Diretor(a) de Secretaria**, em 05/12/2022, às 15:10, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0134303** e o código CRC **5CA939F1**.