



TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

ESTUDO TÉCNICO PRELIMINAR - ETP - TI - 25324351

(para contratação de soluções de TIC por licitação)

Para orientações quanto ao preenchimento do ETP, consultar o Guia de Contratações de TIC do Poder Judiciário ([anexo](#) da Resolução CNJ 468, de 2022) e, subsidiariamente, o Guia Referencial de Preenchimento do ETP do TRF1 (20487579)

ID (PAC):
Esta demanda está prevista no Plano de Contratações Anual — PCA 2026: • Link do PCA: https://www.trf1.jus.br/trf1/compras-licitacoes-e-contratos/plano-de-contratacoes-anual---pca • Id da Futura Contratação: TRF1_DITEC_0018_2026 • Unidade Requisitante: DITEC - DIVISÃO DE TECNOLOGIA. • Classificação: TIC - Serviços de TIC • Descrição: Prorrogação do contrato de suporte técnico para o antimalware/antivírus corporativo da JF1 (ESET)
1. DESCRIÇÃO SUCINTA DA NECESSIDADE
1.1. O presente Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda de suporte especializado ao antivírus , conforme descrito no Documento de Formalização da Demanda - DFD 1ª Região 22194178, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo planejamento.
2. JUSTIFICATIVA EXPRESSA PARA A CONTRATAÇÃO
2.1. Justificativa expressa para a contratação: 2.1.1. O Tribunal Regional Federal da 1ª Região, as Seções e Subseções Judiciárias que compõem a Justiça Federal da Primeira Região lidam diariamente com uma grande diversidade de informações. Em determinadas ocasiões, há que se preservar o seu sigilo e, de forma geral, deve-se assegurar a integridade e disponibilidade das informações. 2.1.2. As soluções de proteção destinadas aos usuários residenciais não são suficientes para as necessidades da Justiça Federal da Primeira Região, visto que não possuem mecanismo centralizado de gerência e seria exigida dos próprios usuários a execução das tarefas de instalação, configuração e atualização do antivírus 2.1.3. A continuidade dos serviços é crítica, uma vez que qualquer interrupção na proteção antivírus compromete a segurança do ambiente tecnológico institucional. A descontinuidade contratual poderia exigir que servidores do TRF1 assumissem a sustentação da solução, o que reduziria a qualidade do suporte, em razão da limitada especialização disponível internamente,

impactando diretamente na segurança das informações judiciais.

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

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

2.1.6. A segurança da informação é uma vertente cada vez mais necessária na composição da gestão de companhias e órgãos públicos, pois para além da crescente complexidade dos sistemas de negócio das empresas existe também uma grande necessidade de proteção dos ativos organizacionais. Em paralelo, cumpre destacar que a indústria do cibercrime é um ramo de negócio cada vez mais promissor e que acarreta em significativos prejuízos para as mais diversas áreas empresariais e governamentais no Brasil e mundo.

2.1.7. 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 suas tentativas de invasão, estão inclusos mecanismos de inteligência artificial e de ocultação para burlarem a detecção de sistemas de segurança, como antimalwares e firewalls.

2.1.8. 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. Estes eventos contribuem para um enorme prejuízo em relação às suas imagens públicas, pois tais entidades prestam serviços à sociedade como um todo e mantêm na sua base inúmeros dados pessoais da população.

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

2.1.10. Tudo isso implica em uma atenção especial ao monitoramento e proteção das estações de trabalho e dos equipamentos servidores da organização, sendo essencial a aquisição de uma ferramenta moderna a fim de evitar pontos de vulnerabilidades na rede. Outro ponto de fundamental importância é que essa ferramenta seja dotada de uma gerência centralizada, de forma que seja possível conduzir a administração de todo o parque antimalware garantindo que as políticas e atualizações ocorram de forma imediata a todos os nós da rede protegida.

2.1.11. Como o término da vigência do Contrato 65/2022 (17107442), firmado com a AX4B Sistemas de Informática Ltda., previsto para 15/02/2025 (1º Termo Aditivo (19974069)), foi realizada a instrução processual a fim de prorrogar o contrato atual. Porém, no momento da formalização do termo aditivo (22100820), verificou-se, em consulta prévia aos cadastros de sanções aplicadas, notadamente o [CEIS](#), CNEP, CNJ e SICAF (22158843), que a

contratada estava impedida de participar de licitações até 12/12/2025. **Dessa forma, o contrato não pôde ser prorrogado** e a Justiça Federal da 1ª Região está sem os serviços de suporte até a presente data.

2.1.12. Deste modo, a contratação do item de suporte especializado na solução é medida que se impõe para continuidade da salvaguarda e segurança do ambiente tecnológico, pois sem o referido serviço os riscos de ataques e suas consequências seriam ainda mais graves, podendo impactar, usuários internos e externos, inclusive os jurisdicionados.

2.1.13. Tal contratação garantirá um atendimento operacional especializado, mais eficiente e contínuo, prevendo monitoramento e manutenção da solução com suporte oficial do fabricante.

2.2. Riscos da não contratação:

2.2.1. Menor agilidade na aplicação de correções especializadas, aumentando a chance de ataques.

2.2.2. Maior risco de erros em atualizações, patches ou implementações.

2.2.3. Maior tempo de resposta e recuperação no caso de incidentes que envolvam a solução.

2.2.4. Maior probabilidade de indisponibilidade de sistemas e serviços críticos que dependam da solução.

2.3. Gerenciamento de riscos:

2.3.1. Conforme a Resolução TRF1 Presi 34/2017, os riscos desta contratação foram mapeados no documento 23802806.

3. ALINHAMENTO COM OS INSTRUMENTOS DE PLANEJAMENTO

3.1. Plano Estratégico de Tecnologia da Informação da Justiça Federal-PETI para 2021-2026, aprovado pela Resolução CJF n. 685/2020.

3.1.1. A ação está alinhada ao planejamento estratégico de TI da JF.

3.1.2. Objetivo estratégico relacionado: 2021-2026 - ID: 1 - Aperfeiçoar e Assegurar a efetividade dos serviços de TI para a Justiça Federal.

3.2. Plano Diretor de Tecnologia da Informação da Justiça Federal da Primeira Região-PDTI-TRF1 2024/2026

(<https://www.trf1.jus.br/trf1/apresentacao/planejamento>).

3.2.1. A ação está alinhada ao plano diretor de TI da JF1

3.2.2. Iniciativa do PDTI relacionada: PDTI-2024-063 - Ampliar a capacidade de gerenciar os riscos de segurança cibernética do ambiente tecnológico

3.3. Plano de Contratação de Soluções de Tecnologia da Informação - PCSTI 2026 (24756232):

3.3.1. A ação está prevista no plano de contratações de soluções de TI da JF1

3.3.2. Ação do PCSTI relacionada: ID 60464 - Prorrogação do Contrato de suporte técnico para o antimalware/antivírus corporativo da JF1 (ESET)

3.4. Plano de Contratação Anual-PCA-2026:

3.4.1. Link do PCA: <https://www.trf1.jus.br/trf1/compras-licitacoes-e-contratos/plano-de-contratacoes-anual----pca>.

3.4.2. Unidade Requisitante: DITEC-DIVISÃO DE TECNOLOGIA.

3.4.3. ID da Futura Contratação: TRF1_DITEC_0018_2026

3.4.4. Classificação: TIC-Serviços de TIC.

3.4.5. Descrição: Prorrogação do Contrato de suporte técnico para o antimalware/antivírus corporativo da JF1 (ESET)

4. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS QUALITATIVOS

4.1. Análise das contratações anteriores

4.1.1. Observou-se, para esse planejamento, a análise das contratações anteriores, de modo a identificar oportunidades de melhoria.

4.1.1.1 Ocorreu aquisição de solução de antivírus, por meio do processo licitatório n.º 24/2022 (16432425), PAe 0013621-23.2021.4.01.8000. O processo gerou ata de registro de preço firmada com a empresa AX4B Sistemas de informática 16871292.

4.1.2. Durante o processo licitatório n.º 24/2022 (16432425), foram apresentados esclarecimentos de várias empresas, que serão detalhados a seguir:

4.1.2.1. Esclarecimento Circular nº 31.2022 - Resposta Esclarec. 01 e 02 (16435256), ocorreram perguntas que englobam os requisitos técnicos:

Pergunta 01: visando garantir maior precisão na formulação da proposta a ser ofertado no presente certame, gostaríamos de solicitar informações a respeito das estimativas em relação às quantidades e periodicidade das solicitações de fornecimento dos itens objetos da contratação. Há um cronograma previsto de fornecimento? Caso não haja, é possível informar se a Administração pretende solicitar o fornecimento, desinstalação, instalação e configuração de licenciamento de todos os equipamentos ativos, simultaneamente?

Resposta 01: Não há previsão assertiva com relação aos quantitativos que serão solicitados inicialmente, pois o requisito depende de disponibilidade orçamentária, bem como fatores de conveniência deste Tribunal. Entretanto diante da necessidade de manter as atualizações de vacina e a segurança do ambiente, há o intuito de aquisição de licenciamento/subscrição para o quantitativo atual do parque constante no Resumo Analítico de Ativos de Infraestrutura, conforme item 6 do Anexo I do Edital.

Pergunta 02: O subitem “5.1.5.42.4. Possibilitar ações de bloqueio na execução de arquivos que possam ser carregados por upload em browsers e clientes de e-mail.” em nosso entendimento possui característica de uma solução de tecnologia de DLP, sendo esta uma funcionalidade totalmente desconexa do item geral da solução 5.1 SOLUÇÃO DE ANTIRUS PARA ESTAÇÕES DE TRABALHO. Entendemos que por se tratar de um projeto com funcionalidades de proteção, detecção e resposta de incidentes em endpoint a funcionalidade descrita neste item não se encaixa nas soluções de tecnologia de proteção e EDR, sendo assim entendemos que o correto dessa funcionalidade seria a proteção e visibilidade-EDR de arquivos executados que foram feitos DOWNLOAD a partir de browsers e clientes de e-mail? Nosso entendimento está correto?

Resposta 02: O item foi revisado e alterado, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

Pergunta 03: Quanto ao item 4.2 do edital, é exigido que “Os serviços de desinstalação, instalação e configuração deverão ser executados, no prazo máximo de 22 (vinte e dois) dias úteis, contados da entrega das licenças.”. Entendemos que esse prazo é inexecutável para qualquer fornecedor que venha a vencer o certame e necessite realizar o serviço de migração/troca de tecnologia, considerando a complexidade do ambiente e pelo volume (quantidade) de licenças. Desta forma, entendemos que este prazo poderá ser flexibilizado devido a quaisquer problemas que possam ocorrer no ambiente computacional da Contratante ou até mesmo eventos imprevistos (pandemias, desastres, acidentes, indisponibilidades) de naturezas diversas. Está correto o nosso entendimento?

Resposta 03: O item foi revisado e alterado, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

Pergunta 04: Quanto a entrega do objeto referente as licenças, entendemos que deverá ser fornecido de forma imediata (recebimento definitivo), em até 10 dias úteis após solicitação do objeto para o licitante vencedor, com a garantia/atualização pelo período de 60 meses e pagamento será feito de forma única em até 15 dias úteis. Está correto o nosso entendimento?

Resposta 04: O item foi revisado e alterado, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

Pergunta 05: Quanto ao item “5.6.2.40.1. Em caso de fornecimento do Sandbox onpremise 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.”Entendemos que o TRF1 aceitará solução baseada em appliance virtual onde funcionará na sua infraestrutura de virtualização, e que esse requisito é aplicado somente para soluções de sandbox baseada em appliance físico. Está correto o nosso entendimento?

Resposta 05: O entendimento está parcialmente correto. Conforme itens 5.2.40 e 5.2.40.1 do Termo de Referência, serão aceitos solução baseada e, appliance virtual desde que a CONTRATADA forneça todos os recursos de infraestrutura necessários para implantação da solução no ambiente do TRF1

Pergunta 06: Quanto ao item “3.1.31 Manter a solução em funcionamento pelo período de 06 meses após o vencimento do contrato, período considerado como de transição ou renovação, sem custo para o Contratante. Durante esse período não serão exigidas as funcionalidades de EDR, Sandbox e atualização dos componentes.”, entendemos que o fornecedor que participar no lote de subscrição deverá fornecer pelo período de 66 meses para atender ao requisito, já que essa modalidade de fornecimento tem por finalidade que o objeto contratado esteja disponível somente no período de contrato e uso. Está correto o nosso entendimento?

Resposta 06: O item foi retirado, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

Pergunta 07: Quanto ao item “3.1.31 Manter a solução em funcionamento pelo período de 06 meses após o vencimento do contrato, período considerado como de transição ou renovação, sem custo para o Contratante. Durante esse período não serão exigidas as funcionalidades de EDR, Sandbox e atualização dos componentes.”, entendemos que a solução ofertada NÃO poderá ter suas funcionalidades básicas (acesso à console de gerenciamento, criação e aplicação de políticas de segurança, acesso a relatórios e atividades diversas de gerenciamento da solução) afetadas após o vencimento do contrato e garantia das licenças. Está correto o nosso entendimento?

Resposta 07: O item foi retirado, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

Pergunta 08: Quanto ao item “5.2.2.42. Deverá apresentar interface para investigação usando funcionalidades de Detecção e Resposta, sendo possível tomar ações para os equipamentos em análise”, entendemos que essa funcionalidade do EDR, muitas vezes considerada como módulo, poderá ser entregue em uma console dedicada para investigação, desde que atenda o requisito. Nosso entendimento está correto?

Resposta 08: O entendimento está incorreto, o gerenciamento de toda solução deve ser único, centralizado e com módulos do mesmo fabricante, conforme itens 5.5.2.2 e 5.5.1.5 do Anexo I do Edital.

Pergunta 09: Quanto ao item “5.6.5.27. Deverá implementar técnicas de Detecção e Resposta (EDR) para prover detecção e investigação para atividades suspeitas”, entendemos que essa funcionalidade será aceita desde que seja compatível para, no mínimo, sistemas operacionais Microsoft (estações e servidores). Nosso entendimento está correto?

Resposta 09: O entendimento está incorreto, conforme o subitens 5.5.5.13 e 5.5.5.1.4 do Anexo I do Edital, a solução de antivírus para estações de trabalho deve ser compatível com sistemas operacionais Linux CentOS e Linux Debian além dos citados

4.1.2.1.1. Observa-se que, esses pedidos de esclarecimento, constavam fundamentados no edital e não causaram sua republicação. Assim, a equipe de planejamento da contratação buscou a melhoria na descrição da especificação técnica para solução.

4.1.2.2. Esclarecimento Circular nº 32.2022 - Resposta Esclarec. 03 e 04 (16435312), ocorreram perguntas que englobam os requisitos técnicos:

Pergunta 01: Com base nos pilares da impessoalidade e isonomia, princípios basilares de todo processo licitatório, a respeito da elaboração independente de Proposta, entendemos que as propostas apresentadas, sejam elaboradas de maneira independente (pelos licitantes) e o conteúdo das mesmas não sejam, no todo ou em parte, direta ou indiretamente, informados, discutidos ou recebidos/compartilhados por quaisquer participantes potenciais ou de fato, utilizando-se quaisquer meios ou pessoas. Está correto o nosso entendimento?

Resposta 01: Está correto o entendimento.

Pergunta 02: [...] entendemos que para resguardar ao TRF1 e Órgãos Participantes sobre a participação de empresas que não possuam especialização necessária, conforme procedimento padrão do processo licitatório, será necessário o envio de Atestado(s) de Capacidade Técnica para comprovação de experiência prévia. Está correto o nosso entendimento?

Resposta 02: Não está correto o entendimento, uma vez que no item 09 do Edital do Pregão em epígrafe, não foi exigido qualificação técnica.

Pergunta 03: Ainda relacionado com o esclarecimento anterior (ESCLARECIMENTO 2) relacionado à experiência prévia, além da comprovação de prestação de serviços de suporte especializado e treinamento, qual será o quantitativo mínimo ou percentual de estações de trabalho e equipamentos servidores contido(s) no(s) Atestado(s) para a

comprovação da especialização das empresas participantes através da capacidade técnica?

Resposta 03: Manifestação na questão anterior.

Pergunta 04: Relacionado com o ITEM 10 - DO JULGAMENTO, tem-se detalhado no subitem 10.3, alínea b, que serão desclassificadas/recusadas as Propostas que não indicarem marca ou mencionarem mais de uma marca para o mesmo item. Nesse sentido, entendemos que o item MARCA está relacionado com o FABRICANTE da Solução ofertada, sendo possível a utilização de MODELOS, ou no caso produtos do mesmo fabricante para atendimento aos itens, nos mesmos moldes do descrito para o cadastramento da proposta (ITEM 4.1 - proposta com a descrição do objeto ofertado, marca, modelo e o preço unitário cada item). Está correto o nosso entendimento?

Resposta 04: Está correto o entendimento, quando no Edital mencionar "marca" entende-se por fabricante/software ofertado, devendo ser indicado na proposta.

Pergunta 05: Relacionado ao ITEM 3.1 do ANEXO I - TERMO DE REFERÊNCIA, temos preconizado que os Grupos 1 e 2 possuem as mesmas especificações técnicas, com os mesmos quantitativos registrados pois tratam-se de tipo de licenciamento distintos que foram assim distribuídos para ampliação da concorrência, que o TRF1 irá homologar somente o lote de menor preço, devendo após aceitação da melhor proposta, cancelar o grupo que restar com o maior valor. Nesse diapasão, entendemos que como licenciamento perpétuo (GRUPO 1), enquadram-se as soluções que sejam licenciadas em nome do TRF1 e/ou demais órgãos participantes e que, mesmo após o seu vencimento, continuem acessíveis e operacionais após a expiração da vigência adquirida (GARANTIA), em consonância com o ITEM 3.1.31. (OBRIGAÇÕES DA CONTRATADA) que versa que a solução em funcionamento seja mantida pelo período de 06 meses após o vencimento do contrato, período considerado como de transição ou renovação, sem custo para o Contratante e que durante esse período de 06 meses, onde não serão exigidas as funcionalidades de EDR, Sandbox e atualização dos componentes. Está correto o nosso entendimento?

Resposta 05: O item foi revisado e alterado, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

Pergunta 06: ...] Como característica do modelo SaaS (Software as a Service), caso específico esse para oferta em Nuvem e que por sua vez não possibilita o LICENCIAMENTO PERPÉTUO, após expirada a vigência é encerrado o acesso ao serviço/instância correspondente e nesse sentido entendemos que, para atendimento do ITEM 3.1.31. (OBRIGAÇÕES DA CONTRATADA - Manutenção da solução em funcionamento pelo período de 06 meses após o vencimento do contrato), as GERÊNCIAS CENTRALIZADAS das ofertas baseadas em Nuvem deverão contemplar período de 66 (sessenta e seis) meses sendo esses compostos pela vigência de 60 meses com o adicional dos 06 meses relativos ao período considerado como de transição ou renovação. Está correto o nosso entendimento?

Resposta 06: O item foi revisado e alterado, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

Pergunta 07: De acordo com detalhado nos itens do GRUPO 1 - ITENS 5.1.2.40., 5.2.2.40., e do GRUPO 2 - ITENS 5.5.2.40. e 5.6.2.40., transcrevemos: ...] Como característica do modelo SaaS (Software as a Service), caso específico esse para oferta em Nuvem e que por sua vez não possibilita o LICENCIAMENTO PERPÉTUO, entendemos que serão aceitas soluções baseadas no modelo de licenciamento em SUBSCRIÇÃO (NUVEM) para os itens relacionados com as exigências de SANDBOX e EDR para os GRUPOS 1 e 2, e cuja garantia técnica detalhada nos itens 5.1.6.10., 5.2.6.10., 5.5.6.10., 5.6.6.10. e 7.1.7., determina que a mesma deve incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia. Está correto o nosso entendimento?

Resposta 07: O item foi revisado e alterado, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

Pergunta 08: Entendemos que no caso de oferta de solução SANDBOX onpremise, a solução ofertada deve contemplar todos os componentes para sua implementação, desde equipamentos físico (HARDWARE) assim como todo o conjunto de software (Virtualizadores, Banco de dados e Sistemas operacionais das Sandbox's, dentre outros) na sua oferta e que os mesmo deverão estar detalhados com a descrição do objeto ofertado, marca e modelo na composição da Proposta a ser apresentada e em consonância com o item 4.1 do Edital. Está correto o nosso entendimento?

Resposta 08: A preferência para o fornecimento do serviço é em nuvem, mas caso o fabricante opte por oferecer on premise, devesse arcar com toda infraestrutura necessária para manter o serviço em funcionamento correto, conforme itens 5.5.2.40 e 5.5.2.40.1 do Anexo I do Edital.

Pergunta 09: Conforme pode se extrair do ITEM 3.1 do ANEXO I - TERMO DE REFERÊNCIA, observa-se a existência das mesmas especificações técnicas para os Grupos 1 e 2 e nesse sentido, relacionados aos itens 5.1.1.2.1.(...), 5.2.1.2.1.(...), 5.5.1.2.1. (...) e 5.6.1.2.1. (...), entendemos que no caso de oferta de gerência centralizada do mesmo fabricante da solução no modelo on-premise, a CONTRATANTE irá disponibilizar máquina virtual para instalação desse componente (gerência centralizada de solução on-premise). Está correto o nosso entendimento?

Resposta 09: O entendimento está correto, para atendimento do item de gerenciamento centralizado será aceita soluções do tipo appliance virtual, conforme item 5.1.1.2.1 do Anexo I do Edital.

Pergunta 10: Mediante as especificações constantes nos itens 5.1.5.1. (...) e 5.5.5.1. (...), temos detalhado a exigência de compatibilidade com os sistemas operacionais Windows 8.1, Windows 10, Linux CentOS e Linux Debian, no entanto, em contraponto com o detalhamento constante no ITEM 6. AMBIENTE TECNOLÓGICO, os sistemas operacionais utilizados nas estações de trabalho detalhados no subitem 6.1.2.1. são Windows 8.1 e Windows 10, informação essa já confirmada na fase de pesquisa de mercado. Entendemos então que as soluções ofertadas para atendimento ao exigido nos itens 5.1.5.1. e 5.5.5.1 deverão ser compatíveis com os sistemas Windows 8.1 e Windows 10, em consonância com o detalhamento do parque tecnológico existente. Está correto o nosso entendimento?

Resposta 10: O entendimento está parcialmente correto. Conforme os itens 5.5.5.1.3 e 5.5.5.1.4 do Anexo I do Edital a solução deve ser compatível também com sistemas operacionais Linux CentOS e Debian. Os itens citados no ambiente tecnológico não são exaustivos.

Pergunta 11: A respeito dos serviços de desinstalação, utilizando como premissa as informações inerentes ao parque computacional e detalhadas no ITEM 6. AMBIENTE TECNOLÓGICO, o software de antivírus atualmente em operação no ambiente é o detalhado no subitem 6.1.2.2., a saber o Antivírus McAfee. Temos detalhado então, nos itens 5.1.3., 5.2.3., 5.5.3. e 5.6.3., que a CONTRATADA deverá realizar os serviços de desinstalação dessa solução e nesse sentido, entendemos que a Gerência dessa solução em funcionamento (Antivírus McAfee) será disponibilizada para que o processo de remoção da ferramenta existente possa ocorrer, sem o advento de eventual reboot ou solicitação de ação do usuário da estação ou servidor. Está correto o nosso entendimento?

Resposta 11: Está correto o entendimento. O item 4.1.17 da Minuta do Contrato - Anexo V do Edital, foi revisado para melhor esclarecimento, devendo ser observado o Edital disponível a partir da presente data nos Portais deste Tribunal e Compras do Governo Federal.

4.1.2.2.1. Assim, a equipe de planejamento da contratação buscou a melhoria na descrição da especificação técnica para solução.

4.1.2.3. Esclarecimento Circular nº 36.2022 -Resposta Esclarecimento 05 (16448402), ocorreram perguntas que englobam os requisitos técnicos:

Pergunta 01: Em relação ao item 5.5.2.22 “Deverá permitir instalação e desinstalação remota dos agentes antivírus, através da console de gerenciamento” Questionamos se a ação solicitada no item 5.5.2.22 poderá ser executada utilizando o Active Directory, ou de forma nativa pela própria solução. Está correto o nosso entendimento?

Resposta 01: O entendimento do item está parcialmente correto. Considerando o disposto no Item 5.2.25, a instalação ou desinstalação poderá ser realizada por meio do Active Directory, via GPO, desde que observado o constante no Item 5.5.4.3 do Anexo I do Edital, referente a requisitos da instalação da solução. No caso suscitado a disponibilização do arquivo de instalação deverá ocorrer por meio da gerência e conter todas as informações pertinentes para que, uma vez instalado nos endpoints, o agente possa se comunicar automaticamente com a gerência.

4.1.2.2.1. Assim, a equipe de planejamento da contratação buscou a melhoria na descrição da especificação técnica para solução.

4.1.2.4. Esclarecimento Circular nº 47.2022 - Resposta Escl. 07 e 08 (16494787), ocorreram perguntas que englobam os requisitos técnicos:

Pergunta 01: Em relação ao ANEXO V (CRONOGRAMA DE DESEMBOLSO RELATIVO AO ITEM 03), entendemos que o mesmo deverá ser apresentado pela CONTRATADA, não havendo necessidade de envio do mesmo como documentação habilitatória do processo licitatório em epígrafe. Está correto o nosso entendimento?

Resposta 01: Não está correto o entendimento, o Cronograma de desembolso constante do Anexo V da Minuta de Contrato será preenchido pela administração do TRF1 por ocasião da assinatura do(s) contrato(s), com base na proposta da Licitante vencedora.

Pergunta 02: Em virtude de resposta de questionamentos anteriores, relacionados com a compatibilidade de plataformas de sistemas operacionais, especificamente no que tange aos sistemas operacionais LINUX, baseado no ITEM 6. AMBIENTE TECNOLÓGICO, subitem 6.1.2. Software utilizados nas estações clientes (6.1.2.1. Windows 8.1 e 10 e 6.1.2.2. Antivírus McAfee), qual o quantitativo de estações clientes que utilizam os sistemas operacionais LINUX?

Resposta 02: Estima-se que o número de estações de trabalho Linux na 1ª Região seja de aproximadamente 20 unidades.

Pergunta 03: Entendemos que serão desclassificadas/recusadas as propostas que não atendam às exigências técnicas obrigatórias, não sendo aceitas soluções personalizadas para o TRF1, devendo a comprovação de atendimento às especificações técnicas mínimas exigidas considerar a última versão de software disponível pelo fabricante na data da licitação, e em consonância ao item 4.4 do Edital. Está correto o nosso entendimento?

Resposta 03: O entendimento está correto. Os componentes deverão estar em suas versões atualizadas e devem ser de autoria do mesmo fabricante, conforme item 5.1.1.5. Não será permitido o desenvolvimento de componentes da solução após a contratação, conforme item 5.1.1.4, impossibilitando soluções personalizadas para o

TRF1. Ainda as comprovações de atendimento técnico deverão considerar a última versão do software, alinhado ao disposto ao item 4.4 do Edital.

Pergunta 04: Ainda em relação ao questionamento anterior, entendemos que não poderá(ão) ser(em) utilizada(s) declaração(ões) do fabricante contraditória(s) às disponíveis na(s) documentação(ões) pública(s) e oficial(is) da última versão de software disponível pelo fabricante na data da licitação e em consonância ao item 4.4 do Edital. Está correto o nosso entendimento?

Resposta 04: A hipótese de apresentação de declaração do fabricante para comprovação de algum item, possibilidade prevista no item 4.2 k.1 do Edital, deve ser utilizada nos casos em que o fabricante não disponha de documentação comprobatória, possível de ser apresentada sob a forma de "manuais, catálogos, folhetos, impressos ou publicações originais do fabricante ou outros documentos suficientes para comprovação dos requisitos técnicos do software ofertado". Para casos omissos na documentação a empresa poderá, por exemplo, fazer o uso de prints de tela da solução de forma a comprovar algum quesito. Ainda as comprovações de atendimento técnico deverão considerar a última versão do software, alinhado ao disposto ao item 4.4 do Edital. Salientamos a prerrogativa prevista no item 8.9 do Edital no sentido da possibilidade de solicitação de esclarecimentos e diligências destinadas a elucidar ou a complementar a instrução do processo e sempre que julgar necessário.

Pergunta 05: De acordo com respostas de questionamentos já publicados, no que concerne à oferta de solução ONPREMISE, entendemos que deverão estar detalhados na Proposta todos os componentes de Hardware (equipamentos físicos) e sua garantia pra os 60 (sessenta) meses, assim como todo o conjunto de software (Virtualizadores, Banco de dados e Sistemas operacionais das Sandbox's, dentre outros) com a descrição do objeto ofertado, marca e modelo em sua oferta. Está correto o nosso entendimento?

Resposta 05: O entendimento está correto. A apresentação da proposta deverá conter detalhamento de todos os itens que compõe a solução ofertada, podendo a administração solicitar esclarecimento e formalização de quaisquer itens que componham a proposta. Para o item 5.1.2.40 caso a solução de Sandbox seja fornecida "onpremise" em appliance físico ou virtual, é necessário que o fornecimento de todos os recursos de infraestrutura para implantação da solução esteja descrito na Proposta.

Pergunta 06: Uma vez que não será exigida experiência prévia das proponentes e nesse sentido, objetivando a resguardar o TRF1 sobre a garantia de funcionamento da solução a ser ofertada, entendemos que no caso de oferta ONPREMISE, deverá ser comprovado que o(s) equipamento(s) ofertado(s) suporte(em) toda a solução a ser instalada, em específico no que diz respeito a capacidade máxima de clientes por gerência(s), e em características mínimas de PROCESSADOR, MEMÓRIA e/ou ESPAÇO EM DISCO por exemplo. Está correto o nosso entendimento?

Resposta 06: No caso de solução on-premisse baseada em appliance físico ou virtual a solução deverá estar licenciada e dimensionada de forma a suportar, no mínimo, a quantidade total de clientes gerenciados objeto do Registro de Preços com todas as funcionalidades da solução habilitadas. A adequação do dimensionamento do(s) equipamento(s) deverão ser objeto de comprovação documental. Esclarecemos que em caso de appliance virtual para o item gerenciamento centralizado, o fornecimento do hardware ficará a cargo do CONTRATANTE, conforme item 5.1.1.2.1 e esclarecimentos anteriores. Esclarecemos, ainda, que nesse caso a garantia técnica se estende a todo o objeto do fornecimento pelo período mínimo de 60 (sessenta) meses.

Pergunta 07: Entendemos que serão aceitas soluções baseadas no modelo de licenciamento em SUBSCRIÇÃO (NUVEM) para os GRUPOS 1 e 2, observados os itens 5.1.6.10., 5.2.6.10., 5.5.6.10., 5.6.6.10. e 7.1.7, que versam que a garantia deva incluir o funcionamento do serviço de sandbox e de detecção e resposta durante todo o período de vigência da garantia, dentre os demais recursos. Está correto o nosso entendimento?

Resposta 07: O entendimento está parcialmente correto. No tocante aos itens 5.1.6.10., 5.2.6.10., 5.5.6.10., 5.6.6.10. e 7.1.7 a garantia deve incluir o funcionamento dos serviços de sandbox e detecção e resposta (EDR) durante o período de vigência. Esclarecemos que os grupos 01 e 02 possuem forma de licenciamento diferente conforme item 3.1 do Anexo I do Edital. Para o grupo 01, as licenças perpétuas concernem apenas a proteção endpoint de estações de trabalho e servidores, vedado o fornecimento por meio de subscrição. Subscrição deverá ser ofertada no Grupo 02, favor observar o subitem 3.1 do Edital.

Pergunta 08: De acordo com o preconizado no item 10.3 do Edital, e subitem, entendemos que serão desclassificadas as propostas que não atendam às exigências técnicas obrigatórias na sua integralidade, ou seja, a TODOS os itens constantes no Termo de Referência. Está correto o nosso entendimento?

Resposta 08: Está correto o entendimento, nos termos do item 10.3 linha "c" do Edital.

4.1.2.4.1. Assim, a equipe de planejamento da contratação buscou a melhoria na descrição da especificação técnica para solução.

4.1.2.5. Esclarecimento Circular nº 48.2022 - Resposta Esclarecimento 09 (16495307), ocorreram perguntas que englobam os requisitos técnicos:

Pergunta 01: Está correto o entendimento, nos termos do item 10.3 linha "c" do Edital.

Resposta 01: No TRF1 aproximadamente 20 estações de trabalho; Na SJMG 0 estações de trabalho (16488237); Na UFT 20 estações de trabalho (16488268).

Pergunta 02: Quanto ao item 5.6.2.40.1 "Em caso de fornecimento do Sandbox onpremise 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.", entendemos que o hardware/servidor/appliance deverá acompanhar os cabos de força e cabo de rede e que o mesmo poderá ficar condicionado no rack/datacenter do TRF1 que disponibilizará a entrega da ligação elétrica para o devido funcionamento do(s) equipamento(s). Nosso entendimento está de acordo?

Resposta 02: Está correto o entendimento.

Pergunta 03: Quanto ao 5.6.3.1."A desinstalação do parque atual existente na JF1 deverá ser efetuada pela CONTRATADA", entendemos que é limitado somente os dispositivos que estão na rede corporativa interna do TRF1. Nosso entendimento está de acordo?

Resposta 03: Está parcialmente correto o entendimento. A desinstalação deve acontecer em todo parque computacional da Justiça Federal da 1ª Região, incluindo TRF1, seções e subseções judiciárias, limitado aos equipamentos instalados na rede interna dessas localidades, com conectividade a partir do TRF1 e registrados na atual solução de antivírus atual, conforme item 6.4 do Anexo I do Edital.

Pergunta 04: Considerando a complexidade das exigências técnicas e que muitas vezes se faz necessário a entrega de serviços e licenças adicionais do mesmo fabricante para atender 100% o termo de referência do edital, serão aceitas uma console única e a partir da mesma poderá ter acesso fácil aos demais componentes que também possui funcionalidades dedicadas na console do componente, mas que fazem parte da mesma solução

Resposta 04: O entendimento está parcialmente correto. Os componentes da solução deverão ser de um único fabricante, vedado soluções que utilizem diversos componentes externos e de outros fabricantes para compor o contexto da solução, como pode ser verificado no que consta no item 5.1.15. Ainda, a solução ofertada deverá estar pronta pra uso, vedado situação que configure implementação ou desenvolvimento de módulos para atender as especificações do edital, conforme item 5.1.1.4. O Gerenciamento Centralizado da solução deve atender ao conjunto completo dos requisitos descritos no item 5.1.2 ou 5.2.2. do Anexo I do Edital e respectivos subitens.

4.1.2.5.1. Assim, a equipe de planejamento da contratação buscou a melhoria na descrição da especificação técnica para solução.

4.1.3. Tabela de itens registrados/adquiridos nas contratações anteriores:

PREGÃO	ARP	CONTRATO	ITEM/DESCRIÇÃO	QUANTIDADE ADQUIRIDA	VENCIMENTOS DAS GARANTIAS
			1 - Solução de antivírus, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses, demais características de acordo com as especificações constantes do Anexo I do Edital. Versão: Eset Protect Enterprise On-Prem 9.1. EDR será entregue On-Premises e o Sandbox em nuvem disponibilizado na nuvem da Eset.	11.800	15/02/2028
			2 - Solução de		

24/2022	24/2022	0048934-11.2022.4.01.8000 - Contrato 65/2022 (17107442)	antivírus, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses, demais características de acordo com as especificações constantes do Anexo I do Edital. Versão: Eset Protect Enterprise On-Prem 9.1. EDR será entregue On-Premises e o Sandbox em nuvem disponibilizado na nuvem da Eset.	1.000	15/02/2028
			3 - Suporte especializado, demais características de acordo com as especificações constantes do Anexo I do Edital.	12 meses	15/02/2025
			4 -Treinamento, demais características de acordo com as especificações constantes do Anexo I do Edital.	10	-
			1 - Solução de antivírus, para estações de trabalho, com garantia e atualização da solução, pelo período de 60 meses, demais características de acordo com as especificações constantes do Anexo I do Edital. Versão: Eset Protect Enterprise On-Prem 9.1. EDR será entregue On-Premises e o Sandbox em nuvem disponibilizado na nuvem da Eset.	1.000 (conforme email 19103180)	22/12/2028
			2 - Solução de		

		0017211-37.2023.4.01.8000 - Contrato 49/2023 (18816820)	antivírus, para equipamentos servidores, com garantia e atualização da solução, pelo período de 60 meses, demais características de acordo com as especificações constantes do Anexo I do Edital. Versão: Eset Protect Enterprise On-Prem 9.1. EDR será entregue On-Premises e o Sandbox em nuvem disponibilizado na nuvem da Eset.	-	-
			3 - Suporte especializado, demais características de acordo com as especificações constantes do Anexo I do Edital.	-	-
			4 -Treinamento, demais características de acordo com as especificações constantes do Anexo I do Edital.	-	-

4.2. Identificação das necessidades de negócio

- 4.2.1. Garantir o maior nível de segurança possível para o ambiente tecnológico da JF1.
- 4.2.2. Centralizar o gerenciamento, promovendo o controle e o monitoramento efetivo da solução em toda a JF1, considerando a disposição geográfica das localidades e estrutura hierárquica da instituição.
- 4.2.3. Prover suporte e atualizações de bases de vacinas, *engines* e quaisquer outros elementos componentes da solução antivírus.
- 4.2.4. Prover suporte técnico especializado concernente a incidentes, problemas, dúvidas de operação, recomendações de mercado e outros detalhes envolvendo a infraestrutura e configuração da solução.

4.3. Identificação das necessidades tecnológicas

- 4.3.1. O serviço de suporte especializado deverá ser prestado para as 13.800 licenças do antivírus ESET PROTECT Enterprise On-Prem (ESET Endpoint & Server Security, ESET Full Disk Encryption, ESET Inspect e ESET LiveGuard Advanced for Endpoint Security + Server Security), atualmente em uso na JF1,

conforme especificações técnicas no ANEXO I - Especificações Técnicas.

4.4. Demais requisitos necessários e suficientes à escolha da solução de TI

4.4.1. Identificação de critérios e práticas sustentáveis

4.4.1.1. Por se tratar de contratação de empresa especializada na prestação de **suporte especializado de antivírus** não havendo oferta de produto por meio físico, observadas as normas vigentes relativas ao desenvolvimento sustentável nas licitações e contratações públicas, bem como o Plano de Sustentabilidade do Tribunal Regional Federal da 1ª Região (PORTARIA PRESI 340/2021), disponível no sítio: <https://portal.trf1.jus.br>, não vislumbramos exigência que possa ser prevista no edital ou no contrato compatível ao objeto desde termo.

4.4.2. Identificação de critérios de acessibilidade

4.4.2.1. A equipe de planejamento não vislumbrou a necessidade de exigências especiais em cumprimento dos critérios de acessibilidade.

4.4.3. Contratações correlatas e/ou interdependentes

4.4.3.1. Contrato n. 65/2022 (17107442), celebrado com a empresa **AX4B SISTEMAS DE INFORMÁTICA LTDA.**

4.4.3.1.1. Vigência: 15/02/2025, conforme 1º Termo Aditivo (19974069) ao Contrato n. 65/2022 (23166914).

4.4.3.2. Contrato n. 49/2023 (18816820), celebrado com a empresa **AX4B SISTEMAS DE INFORMÁTICA LTDA.**

4.4.3.1.2. Vigência: 22/12/2028.

4.4.4. Requisitos legais

4.4.4.1. Leis e Decretos:

a) [Lei Complementar nº 123/2006](#) - Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte c/c [Decreto nº 8.538/2015](#) - altera dispositivos das Leis nº 8.212 e 8.213, ambas de 24 de julho de 1991, da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, da Lei nº 10.189, de 14 de fevereiro de 2001, da Lei Complementar nº 63, de 11 de janeiro de 1990; e revoga as Leis nº 9.317, de 5 de dezembro de 1996, e 9.841, de 5 de outubro de 1999.

b) [Lei nº 13.709/2018](#) - Lei Geral de Proteção de Dados Pessoais (LGPD).

c) [Lei nº 14.133/2021](#) - Lei de Licitações e Contratos Administrativos.

4.4.4.2. Normas específicas para contratações de TI:

a) [Instrução Normativa nº 65/2021 SGD/ME](#) - Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

b) [Instrução Normativa nº 58/2022 SGD/ME](#) - Dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP, para a aquisição de bens e a contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital.

c) [Instrução Normativa nº 81/2022 SEGES/ME](#) - Dispõe sobre a

elaboração do Termo de Referência - TR, para a aquisição de bens e a contratação de serviços, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema TR digital.

d) [Instrução Normativa nº 94/2022 SGD/ME](#) - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

e) [Portaria nº 6.680 SGD/MGI](#) - Altera a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, que estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

4.4.4.3. Normas do Conselho Nacional de Justiça:

a) [Resolução CNJ nº 347/2020](#) - Dispõe sobre a Política de Governança das Contratações Públicas no Poder Judiciário.

b) [Resolução CNJ nº 363/2021](#) - Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.

c) [Resolução CNJ nº 370/2021](#) - Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

d) [Resolução CNJ nº 396/2021](#) - Estabelece a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)

e) [Resolução CNJ nº 468/2022](#) - Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça.

f) [Portaria CJF nº 96/2023](#) c/c [Resolução CNJ nº 400/2021](#) - Dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.

4.4.4.4. Normas do Conselho de Justiça Federal:

a) Resolução 851/2023 c/c [Resolução CJF nº 685/2020](#) - Dispõe do Plano Estratégico de Tecnologia da Informação da Justiça Federal (PETI) para 2021-2026.

b) [Resolução CJF nº 687/2020](#) - Dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus.

c) [Resolução CJF nº 709/2021](#) c/c [Portaria CJF nº 96/2023](#) - Dispõe sobre a Política de Sustentabilidade da Justiça Federal - PSJF e o Manual de Sustentabilidade nas Compras e Contratações do Conselho da Justiça Federal - 2ª Edição

d) [Portaria CJF nº 232/2023](#) - Dispõe sobre as etapas do planejamento das contratações de bens e serviços fundamentadas por meio da Lei n. 14.133, de 1º de abril de 2021, no âmbito do Conselho da Justiça Federal.

e) [Resolução CJF nº 477/2018](#) - Dispõe sobre a Política de Nivelamento de Infraestrutura de Tecnologia da informação da Justiça Federal.

f) [Resolução CJF 842/2023](#) - Dispõe sobre o Plano de Contratações Anual e sobre o Plano de Contratações Compartilhadas Anual, no

âmbito do Conselho e da Justiça Federal de 1º e 2º graus.

4.4.4.5. Normas da Justiça Federal da 1ª Região:

- a) [Resolução PRESI nº 34/2017](#) - Institui a Gestão de Riscos na Justiça Federal de 1º e 2º graus da 1ª Região.
- b) [Resolução PRESI nº 18/2024](#) - Estabelece diretrizes e procedimentos para a elaboração, divulgação e acompanhamento do Plano de Contratações Anual e do Calendário Anual de Contratações e institui o Sistema do Plano de Contratações Anual no âmbito do Tribunal Regional Federal da 1ª Região e das seções judiciárias vinculadas.
- c) [Resolução PRESI nº 36/2021](#) - Institui a Política de Governança e Gestão das Contratações da Justiça Federal da 1ª Região.
- d) Portaria PRESI n. 49/2021- Institui a Política de Proteção de Dados

4.4.5. Requisitos de manutenção:

4.4.5.1. Manutenção preventiva:

- 4.4.5.1.1. Atualizações de segurança: Disponibilização contínua de atualizações de definições de vírus e malware;
- 4.4.5.1.2. Patches de software: Fornecimento de patches corretivos conforme ciclo de vida do fabricante;
- 4.4.5.1.3. Atualizações de versão: Acesso a versões menores e maiores durante a vigência do contrato;
- 4.4.5.1.4. Frequência: Mensalmente ou conforme criticidade identificada.

4.4.5.2. Manutenção corretiva:

- 4.4.5.2.1. Suporte técnico: Disponível em regime 8x5, de segunda a sexta-feira, entre 09h00 e 18h00;
- 4.4.5.2.2. Tempo de resposta: Conforme matriz de severidade definida no ANEXO I - ESPECIFICAÇÕES TÉCNICAS;
- 4.4.5.2.3. Resolução: Conforme matriz de severidade definida no ANEXO I - ESPECIFICAÇÕES TÉCNICAS;
- 4.4.5.2.4. Escalação: Disponibilidade de suporte especializado do fabricante quando necessário.

4.4.5.3. Relatórios:

- 4.4.5.3.1. Mensal: Relatório de chamados abertos, classificação de severidade, problemas abordados e ações realizadas;
- 4.4.5.3.2. Trimestral: Health Check da plataforma de segurança com análise de configurações e recomendações;
- 4.4.5.3.3. Anual: Relatório de efetividade da solução e recomendações de otimização.

4.4.5.4. O atendimento do suporte, incluindo telefone, e-mail ou outros que se fizerem necessários, deverá ser realizado no idioma português do Brasil.

4.4.5.5. Os serviços deverão ser contratados diretamente com o fabricante do software disponibilizado no Contratante, que atuará como intermediário para acionamento dos serviços.

- 4.4.5.5.1. Tal exigência é prática usual de mercado, está aderente as últimas contratações realizadas por este órgão e justifica-se diante da necessidade de especialização na solução, posto que no caso de softwares em geral, a atualização é desenvolvida e disponibilizada

exclusivamente pelo fabricante, pois envolve fornecimento de bases de vacinas, *engines*, upgrades e quaisquer outros elementos componentes que integram o software antivírus, bem como somente o fabricante possui competência para resolução de problemas mais complexos de configuração e/ou disponibilidade da solução.

4.4.5.6. Demais requisitos de manutenção estão detalhados no ANEXO I - Especificações Técnicas.

4.4.6. Requisitos temporais:

4.4.6.1. O prazo de vigência da contratação iniciar-se-á na data da assinatura do contrato e estender-se-á, impreterivelmente, até a data limite de 16/12/2027, momento em que expira o direito de uso das licenças das soluções ESET em produção no âmbito do TRF1.

4.4.6.1.1. Diante da vinculação estrita do serviço de suporte ao ciclo de vida das licenças ativas, não caberá qualquer espécie de prorrogação deste contrato para além da data fixada no subitem 16.1, restando caracterizada a exaustão do objeto nesta data.

4.4.6.1.2. O faturamento e o pagamento dos serviços observarão rigorosamente a proporcionalidade dos meses (e fração de dias no mês de encerramento) efetivamente executados a partir da Ordem de Início dos Serviços, não havendo obrigação de pagamento por período anterior à efetiva prestação.

4.4.7. Requisitos de segurança:

4.4.7.1. Os serviços prestados devem adequar-se às necessidades de negócio e técnicas estabelecidas pela segurança do Tribunal. É necessário considerar a infraestrutura existente, bem como sua integração eficiente.

4.4.7.2. Para a formalização de eventual contratação, faz-se necessário que seja exigida a assinatura de termo de responsabilidade e sigilo das informações que eventualmente sejam trocadas entre Fornecedor e TRF1. Tal termo deve exigir manifestação da contratada quanto à guarda, privacidade e o sigilo das informações que venham a ter conhecimento em razão do exercício de suas atividades bem como das informações disponibilizadas pela entidade contratante.

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

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

4.4.7.4.1. Obriga-se também a comunicar à Administração, em até 03(três) dias úteis, contadas do instante do conhecimento, a ocorrência de acessos não autorizados a dados pessoais, de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou de qualquer outra forma de tratamento inadequado, suspeito ou ilícito, sem prejuízo das medidas previstas no art. 48 da Lei 13.709/2018 (LGPD).

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

4.4.7.6. É vedado, na execução do ajuste, revelar, copiar, transmitir, reproduzir, transportar ou utilizar dados pessoais ou informações sigilosas a que tiver acesso prepostos, empregados ou colaboradores direta ou indiretamente envolvidos na realização de serviços, produção ou fornecimento de bens. Para tanto, devem ser observados as medidas e os procedimentos de segurança das informações resultantes da aplicação da Lei 13.709/2018 (LGPD) e do parágrafo único do art. 26 da Lei 12.527/2011.

4.4.7.7. Em razão do vínculo mantido, na hipótese de dano patrimonial, moral, individual ou coletivo decorrente de violação à legislação de proteção de dados pessoais ou de indevido acesso a informações sigilosas ou transmissão destas por qualquer meio, a responsabilização dar-se-á na forma da Lei 13.709/2018 (LGPD) e da Lei 12.527/2011.

4.4.7.8. Extinto o ajuste ou alcançado o objeto que encerre tratamento de dados, estes serão eliminados, inclusive toda e qualquer cópia deles porventura existente, seja em formato físico ou digital, autorizada a conservação conforme as hipóteses previstas no art. 16 da Lei 13.709/2018 (LGPD).

4.4.7.9. Não haverá tratamento específico de dados pessoais para esta contratação.

4.4.8. Requisitos de capacitação:

4.4.8.1. Não se aplica.

5. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

5.1. O levantamento do quantitativo leva em consideração o parque atual de licenças de antivírus da JF1:

5.1.1. Contrato 65/2022 (17107442) 12.800 licenças

5.1.2. Contrato 49/2023 (18816820) 1.000 licenças

5.1.3. Totalizando 13.800 licenças.

DESCRIÇÃO DOS BENS E SERVIÇOS	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA																																				
Suporte especializado a 13.800 licenças perpétuas do antivírus ESET PROTECT Enterprise On-Prem (ESET Endpoint & Server Security, ESET Full Disk Encryption, ESET Inspect e ESET LiveGuard Advanced for Endpoint Security + Server Security)	Mês	A quantidade de meses, para a contratação pretendida, deve respeitar o prazo de validade das licenças conforme quadro abaixo: <table><tr><th>NOME DO MÓDULO</th><th>UNIDADES</th><th>SU...</th><th>STA...</th><th>VALIDADE</th><th>TIPO DE ASSINATURA</th></tr><tr><td></td><td></td><td></td><td>✓</td><td></td><td></td></tr><tr><td>ESET LiveGuard Advanced for En...</td><td>9708/12800</td><td></td><td>✓</td><td>16 de dezembro de 2027 20:59:59</td><td>Negócios</td></tr><tr><td>ESET Inspect</td><td>11296/12800</td><td></td><td>✓</td><td>16 de dezembro de 2027 20:59:59</td><td>Negócios</td></tr><tr><td>ESET Full Disk Encryption</td><td>0/12800</td><td></td><td>✓</td><td>16 de dezembro de 2027 20:59:59</td><td>Negócios</td></tr><tr><td>ESET Endpoint & Server Security</td><td>11221/12800</td><td></td><td>✓</td><td>16 de dezembro de 2027 20:59:59</td><td>Negócios</td></tr></table> Assim, deverá se considerado o prazo de vigência limite até a data 16/12/2027.	NOME DO MÓDULO	UNIDADES	SU...	STA...	VALIDADE	TIPO DE ASSINATURA				✓			ESET LiveGuard Advanced for En...	9708/12800		✓	16 de dezembro de 2027 20:59:59	Negócios	ESET Inspect	11296/12800		✓	16 de dezembro de 2027 20:59:59	Negócios	ESET Full Disk Encryption	0/12800		✓	16 de dezembro de 2027 20:59:59	Negócios	ESET Endpoint & Server Security	11221/12800		✓	16 de dezembro de 2027 20:59:59	Negócios
NOME DO MÓDULO	UNIDADES	SU...	STA...	VALIDADE	TIPO DE ASSINATURA																																	
			✓																																			
ESET LiveGuard Advanced for En...	9708/12800		✓	16 de dezembro de 2027 20:59:59	Negócios																																	
ESET Inspect	11296/12800		✓	16 de dezembro de 2027 20:59:59	Negócios																																	
ESET Full Disk Encryption	0/12800		✓	16 de dezembro de 2027 20:59:59	Negócios																																	
ESET Endpoint & Server Security	11221/12800		✓	16 de dezembro de 2027 20:59:59	Negócios																																	

6. ANÁLISE DE SOLUÇÕES POSSÍVEIS

6.1. Identificação das soluções

Cenário nº	Solução	Descrição das alternativas de solução disponíveis no mercado	Fontes de consulta	Link das consultas
1	-	Prorrogação do item 3 (suporte especializado) do contrato n. 65/2022	Contrato TRF1	17107442
2	1	Contratação de suporte especializado para a solução de antivírus pelo período de 12 meses.	B3ware Acorp Future	24692000 24692003 24691965
	2	Contratação de suporte especializado para a solução de antivírus pelo período de 24 meses.	B3ware Acorp Future	24692000 24692003 24691979
	3	Contratação de suporte especializado para a solução de antivírus pelo período de 36 meses.	TRF6 B3ware Acorp Future	23751845 e 23751846 24692000 24692003 24691986
3		Contratação de licença de uso (subscrição) com garantia técnica, atualização e suporte especializado pelo período de 60 (sessenta) meses.	SJRJ Serviço de Saneamento CRT4	23893791 23893802 23893815

6.2. Análise comparativa de soluções

6.2.1. Cenário 1 - Prorrogação do item 3 (suporte especializado) do contrato n. 65/2022 (17107442) firmado com a empresa **AX4B SISTEMAS DE INFORMÁTICA LTDA**

6.2.1.1. O suporte especializado consiste essencialmente na realização de procedimentos destinados a apoiar a equipe de TIC da JF1 na administração da solução, instalação e configuração de módulos e demais componentes, resposta a incidentes, obtenção de evidências, levantamento de informações do ambiente e esclarecimento de dúvidas. Além do acompanhamento nos chamados escalados para a fabricante em situações de falhas/problemas desconhecidos pelo suporte técnico da licitante ou bugs.

6.2.1.2. O referido contrato trata do fornecimento, desinstalação, instalação e configuração de licenças de solução **antivírus**, incluindo garantia, atualização de versões, além de serviços de suporte especializado e treinamento para estações de trabalho e servidores.

6.2.1.3. Dentre as vantagens da renovação do contrato estão:

6.2.1.4.1. Garantia de continuidade do serviço sem interrupções, fundamental para manter a segurança dos sistemas e dados.

6.2.1.4.2. Manutenção de uma relação já consolidada com o fornecedor, que possui conhecimento técnico aprofundado do ambiente de TI da instituição.

6.2.1.4.3. Benefício econômico imediato ao manter as condições contratuais vigentes, que já foram avaliadas como vantajosas em processos anteriores.

6.2.2. Cenário 2 - Contratação de suporte especializado para a solução de antivírus

6.2.2.1. Uma nova contratação de empresa, para prestar os serviços de suporte especializado ao antivírus, visa atender à segurança cibernética

para proteger seus ativos, dados e sistemas contra ameaças digitais emergentes, mantendo atendimento operacional especializado, mais eficiente e contínuo.

6.2.2.2. A finalidade desta é prover o Contratante de solução com vistas a mitigar o risco de infestação das estações de trabalho e equipamentos servidores por ameaças virtuais, bem como manter o controle das estações de trabalho com antivírus atualizado.

6.2.2.3. O serviço de suporte deverá incluir a implementação e operacionalização das atualizações fornecidas pelo fabricante, bem como a manutenção contínua da solução antivírus, com garantia integral dos serviços prestados.

6.2.2.4. Dentre as soluções viáveis para atender ao cenário 2 é possível realizar a contratação com os seguintes prazos: 12, 24 e 36 meses.

6.2.3. Cenário 3 - Contratação de licença de uso (subscrição) com garantia técnica, atualização e suporte especializado pelo período de 60 (sessenta) meses

6.2.3.1. O presente cenário visa à contratação de solução de segurança cibernética por meio do **fornecimento de licenças de software antivírus corporativo**, incluindo **serviços de garantia, suporte técnico especializado e atualização contínua das assinaturas pelo período de 60 meses**.

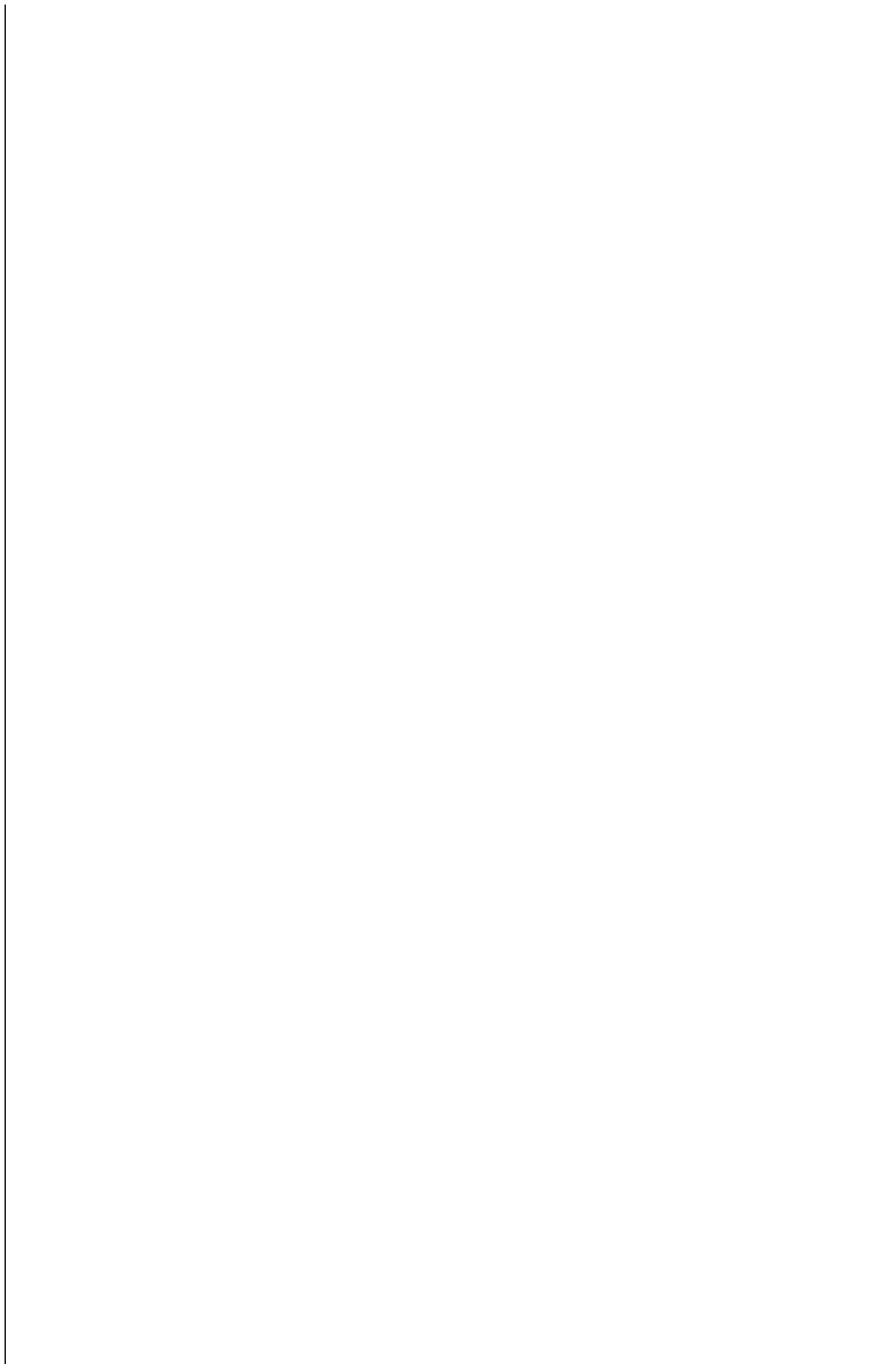
6.2.3.2. A vigência de **60 meses** tem por finalidade garantir **continuidade da proteção e estabilidade orçamentária**, evitando interrupções de cobertura e a necessidade de renovações frequentes, o que pode representar riscos operacionais e de segurança.

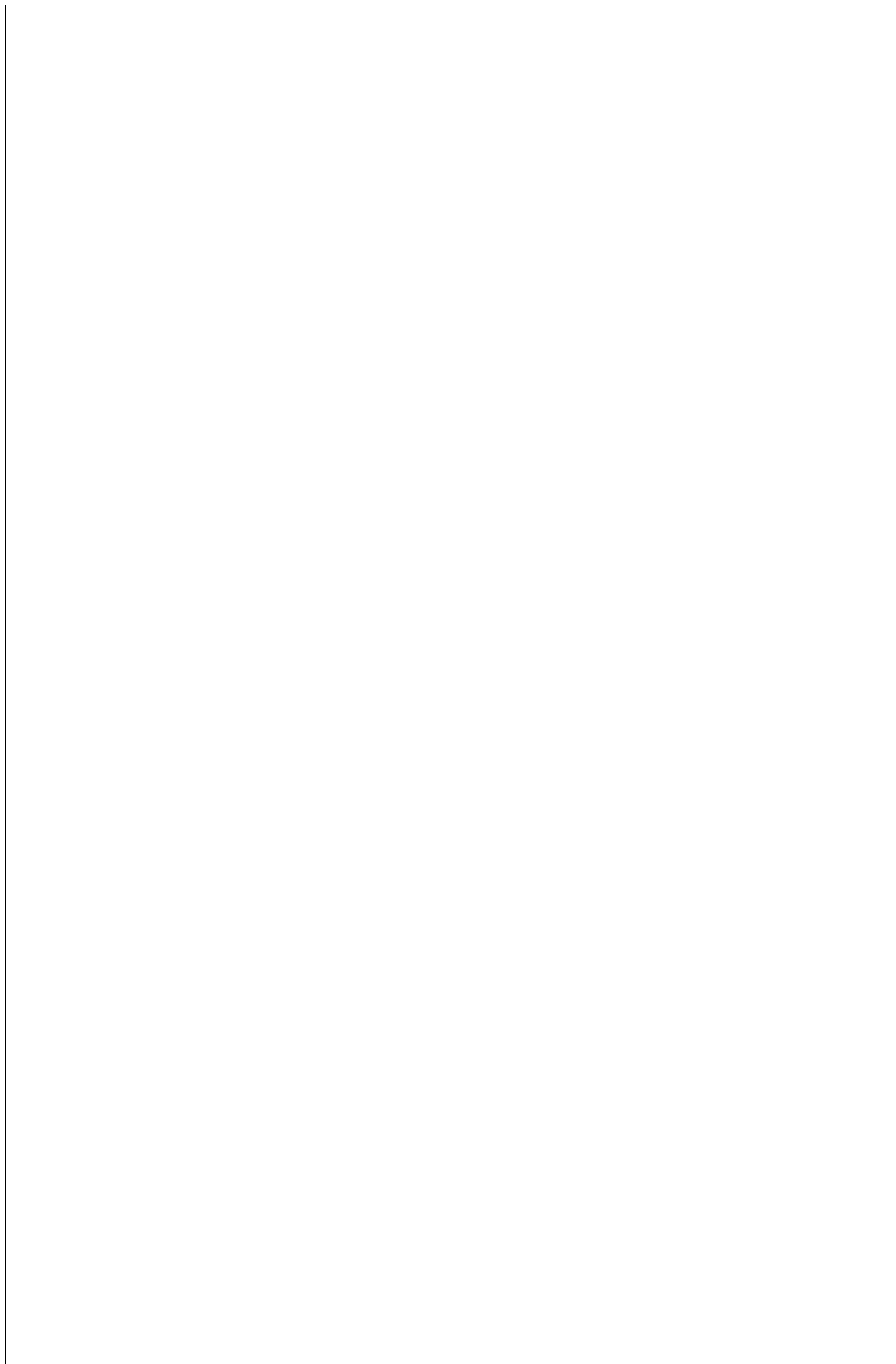
6.2.3.3. A solução tem como objetivo **proteger os ativos tecnológicos** (estações de trabalho, servidores e demais dispositivos conectados à rede) contra ameaças digitais como vírus, ransomware, trojans, phishing, spywares e outras formas de código malicioso que possam comprometer a integridade, confidencialidade e disponibilidade das informações institucionais.

6.2.4. O quadro seguinte poderá auxiliar na comparação de alguns requisitos entre as soluções identificadas.

REQUISITOS	ID DO CENÁRIO	SIM	NÃO	NÃO SE APLICA
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	Cenário 01	X		
	Cenário 02	X		
	Cenário 03	X		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	Cenário 01	X		
	Cenário 02	X		
	Cenário 03	X		
A Solução está disponível no Portal do Software Público Brasileiro?	Cenário 01		X	
	Cenário 02		X	
	Cenário 03		X	
A Solução é um software livre ou software público?	Cenário 01		X	
	Cenário 02		X	
	Cenário 03		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	Cenário 01			X
	Cenário 02			X

A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Cenário 01			X
	Cenário 02			X
	Cenário 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?	Cenário 01			X
	Cenário 02			X
	Cenário 03			X





7. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

7.1. Cenário 1 - Prorrogação do item 3 (suporte especializado) do contrato n. 65/2022 (17107442):

7.1.1. Foi realizada a instrução processual a fim de prorrogar o contrato atual 0048934-11.2022.4.01.8000, porém no momento da formalização do termo aditivo (22100820), verificou-se, em consulta prévia aos cadastros de sanções aplicadas, notadamente o [CEIS](#), CNEP, CNJ e SICAF (22158843), que a contratada foi sancionada com o impedimento de licitar e contratar até 12/12/2025. Dessa forma o contrato não poderá ser prorrogado.

7.1.2. Sendo assim a equipe de planejamento **considerou o cenário inviável**.

8. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

8.1. Cálculo dos custos totais de propriedade

8.1.1. Cálculo dos custos totais de propriedade:

8.1.1.1. Custo Total de Propriedade – TCO (*Total Cost of Ownership*) é o cálculo geral de todos os custos que envolvem a aquisição de um serviço ou produto. Tem como objetivo calcular os custos de vida e aquisição de um produto ou ferramenta e, por fim, determinar se um investimento vale a pena ou não.

8.1.1.2. Conforme inciso III do art. 11 da IN nº 94/2022, uma análise comparativa de custos deverá considerar apenas as soluções técnicas e funcionalmente viáveis, nos seguintes termos:

III - análise comparativa de custos, que deverá considerar apenas as soluções técnica e funcionalmente viáveis, incluindo:

a) cálculo dos custos totais de propriedade (**Total Cost Ownership** - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição

dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento;

b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados

8.2. Mapa comparativo dos cálculos totais de propriedade (TCO)

ESUMO DE CÁLCULO TOTAL DE PROPRIEDADE (TCO)							
CENÁRIO	DESCRIÇÃO	TCO 1º ANO	TCO 2º ANO	TCO 3º ANO	TCO 4º ANO	TCO 5º ANO	MEMÓRIA DE CÁLCULO
2	Contratação de suporte especializado ao antivírus pelo período de 12 meses	R\$ x 12 = R\$	-	-	-	-	Total para 12 meses: R\$ Considerando o menor valor conforme o item 6.3.1.3.2.
	Contratação de suporte especializado ao antivírus pelo período de 20 meses	R\$ x 12 = R\$	R\$ x 8 R\$	-	-	-	Total para 20 meses: R\$ Considerando o menor valor conforme o item 6.3.1.3.2.
	Contratação de suporte especializado ao antivírus pelo período de 36 meses	R\$ x 12 = R\$	R\$ x 12 = R\$	R\$ x 12 = R\$	-	-	Total para 36 meses: R\$ Considerando o menor valor conforme o item 6.3.1.3.2.
3	Contratação de licença de uso (subscrição) com garantia técnica, atualização e suporte especializado pelo período de 60 (sessenta) meses					R\$	Total para 60 meses: R\$ R\$ Conforme subitem 6.3.2.2. deste estudo.

9. ANÁLISE TÉCNICA E ECONÔMICA DAS SOLUÇÕES VIÁVEIS

9.1. Cenário 02: Contratação de suporte especializado ao antivírus pelo período de 20 meses

9.1.1. Este cenário atende aos requisitos de negócio e garante a continuidade dos serviços de suporte especializado ao antivírus, alinhando segurança, continuidade operacional e eficiência econômica.

9.1.2. A quantidade de meses, para a contratação pretendida, deve respeitar o prazo de validade das licenças que conforme o item 5 tem prazo de vigência de até 16/12/2027.

9.1.3. Após avaliação econômica, esse cenário se mostrou o mais economicamente viável, assim sendo o cenário escolhido para esta demanda.

9.2. Cenário 03: Contratação de licença de uso (subscrição) com garantia técnica, atualização e suporte especializado pelo período de 60 (sessenta)

meses

9.2.1. Este cenário atende aos requisitos de negócio e garante a continuidade dos serviços, porém após avaliação economia no item 8.2, o cenário se mostrou menos economicamente viável.

9.3. A equipe responsável, ciente das regras e diretrizes da Resolução CNJ nº 468/2022, após a conclusão de todos os estudos técnicos preliminares aqui contidos, declara ser viável a contratação pretendida.

10. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

10.1. Transição contratual

10.1.1. Não se aplica.

10.2. Adequações do ambiente do órgão impostas pela solução escolhida

Relacionar, quando for o caso, as adequações no ambiente do órgão que precisarão ser providenciadas previamente à implantação e/ou posteriormente visando a operacionalização da solução avaliada, observando-se os seguintes aspectos:

1. Infraestrutura tecnológica, elétrica e de ar-condicionado atual atende? () Sim () Não (X) Não se aplica.

2. Há no Tribunal espaço físico e logística (sala para alocação da mão-de-obra residente, áreas de circulação, espaços de armazenamento dos equipamentos, disponibilidade de equipamentos para uso da contratada, etc.) suficientes para implantação da solução ? () Sim () Não (X) Não se aplica.

3. Há necessidade e disponibilidade de acesso aos sistemas de informação? (X) Sim () Não () Não se aplica.

4. Haverá necessidade de capacitação de servidores para operacionalização da solução escolhida? () Sim (X) Não () Não se aplica.

5. Haverá impacto nas rotinas e processos de trabalho? () Sim (X) Não () Não se aplica.

6. A solução está aderente às normas de segurança adotadas pela JF1? (X) Sim () Não () Não se aplica.

10.3. Demonstração de que o mercado atende aos requisitos mínimos

10.3.1. Não se aplica

10.4. Aplicação de cotas a microempresas (ME) e empresas de pequeno porte (EPP)

10.4.1. Observa-se que a contratação não se trata de bens divisíveis, assim não se aplica a reserva de cota para ME/EPP.

10.5. Parcelamento da solução

10.5.1. Não se aplica

10.6. Descrição integral da solução

10.6.1. Contratação de serviço de suporte técnico especializado na solução **ESET PROTECT Enterprise On-Prem**, atualmente instalada e configurada em toda a Justiça Federal da 1ª Região.

10.7. Benefícios diretos

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

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

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

10.7.4. 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.

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

10.7.6. 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.

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

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

10.8. Benefícios indiretos

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

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

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

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

10.9. Ciclo de vida

10.9.1. A avaliação do ciclo de vida do objeto visa assegurar a escolha da solução que melhor atenda às necessidades do TR1 e proporcione a perfeita execução do objeto contratado. Em conformidade com o art. 9º, III, da Instrução Normativa SEGES/ME nº 81 de 2022, o ciclo de vida do serviço de suporte especializado, podendo variar de acordo com as políticas e procedimentos da empresa responsável pela venda e suporte do software adquirido.

10.9.2. O ciclo de vida pode seguir as seguintes etapas:

10.9.2.1. **Compra ou Renovação:** O ciclo começa com a compra inicial do serviço. Nesta fase, adquire-se o direito de atualização e manutenção das licenças de antivírus em uso na JF1 (escopo do contrato inicial).

10.9.2.2. **Suporte Técnico Especializado:** Durante o período vigência do contrato, há o direito ao suporte técnico especializado para atualizações do software, tais como atualizações e correções de bugs sem custos adicionais, além da operacionalização de todos os componentes da solução, conforme descrito no ANEXO I.

10.9.3. Essas são as principais fases do ciclo de vida do serviço. É importante ressaltar que políticas e termos específicos do ciclo de vida podem variar entre diferentes fornecedores ou revendas do serviço. Portanto, é sempre recomendável analisar os contratos e informações fornecidas pelo fornecedor do antivírus para entender claramente os detalhes do ciclo de vida e as opções disponíveis.

10.10. Outras informações da solução a ser contratada

10.10.1. Modalidade e Tipo de licitação

10.10.1.1. Recomenda-se que esta licitação seja efetuada nos moldes de **PREGÃO ELETRÔNICO** conforme disposto no inciso I, art. 28 da Lei 14.133, de 01 de abril de 2021, visto se tratar de aquisição de serviço comum, cujos padrões de desempenho e qualidade podem ser objetivamente definidos no edital, por meio de especificações usuais de mercado.

10.10.1.2. Para o objeto tratado neste ETP, não há ponderação de qualidade técnica das propostas que excedam os requisitos mínimos, de forma que o critério de julgamento será pelo **MENOR PREÇO**.

10.10.2. Natureza da contratação

10.10.2.1. O objeto da contratação é de natureza contínua, uma vez que trata-se de um serviço essencial e necessário para a administração pública, cuja interrupção prejudicaria a segurança do ambiente tecnológico da JF1.

10.10.3. Condições de participação

10.10.3.1. Será assegurada a participação de empresas reunidas em consórcio, nos termos do art. 15 da Lei n. 14.133/2021.

10.10.3.2. Será admitida a participação de profissionais sob a formade cooperativa, de acordo com o previsto no art. 16 da Lei n. 14.133/2021.

10.10.4. Subcontratação

10.10.4.1. É admitida a subcontratação parcial do objeto, nas seguintes condições:

10.10.4.11. É vedada a subcontratação completa ou da parcela principal do objeto da contratação.

10.10.4.12. A subcontratação fica limitada a prestação do serviço de suporte técnico especializado por parte do fabricante da solução.

10.10.4.2. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à subcontratação.

11. ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO

ITEM	DESCRIÇÃO	QUANTIDADE	UNIDADE DE MEDIDA	VALOR MENSAL	VALOR TOTAL
1	Serviço de suporte técnico especializado para 13.800 licenças de antivírus	20	mês	R\$	

12. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

12.1. A equipe responsável pelo planejamento da contratação, ciente das regras e diretrizes da Resolução CNJ nº 468/2022, após a conclusão de todos os estudos técnicos preliminares aqui contidos, declara ser viável a contratação pretendida.

12.2. As questões elencadas no presente estudo estabeleceram critérios de razoabilidade, eficiência, legalidade, especificações, preço estimado e o princípio da economicidade para a administração pública.

13. APROVAÇÃO E ASSINATURA

Integrante técnico: O presente planejamento foi elaborado em harmonia com a Instrução Normativa nº 94/2022 da SGD/ME, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades de negócio. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade — os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a contratação. Juarez de Oliveira Integrante Técnico Marina Alves Ferreira Integrante Técnico
Integrante demandante: O presente planejamento foi elaborado em harmonia com a Instrução Normativa nº 94/2022 da SGD/ME, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades de negócio. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade — os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a contratação. Luiz Alberto Lima da Costa Integrante Requisitante
Autoridade máxima da área de TI: O presente planejamento foi elaborado em harmonia com a Instrução Normativa nº 94/2022 da SGD/ME. Encontra-se em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades de negócio, atende adequadamente às demandas formuladas pelas áreas envolvidas, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis, pelo que aprovo o artefato e encaminho para prosseguimento da contratação. Janderson Casado de Vasconcelos Santos Diretor da Secretaria de Tecnologia da Informação

ANEXO I ESPECIFICAÇÕES TÉCNICAS

1. SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO

1.1. O serviço de suporte técnico especializado terá seu prazo de vigência iniciado a partir da assinatura do contrato e perdurará, como termo limite e inultrapassável, até a data de 16/12/2027. Esta data marca a expiração das licenças objeto deste suporte, de modo que o pagamento pelo serviço ocorrerá de forma mensal e proporcional apenas durante o período em que o contrato permanecer ativo.

1.2. O serviço deve incluir a operacionalização de todos os componentes da solução, assim como gestão e aplicação das atualizações do fabricante, serviços de manutenção, resolução de problemas e implementações de ações de segurança, com garantia completa dos serviços prestados.

1.2.1. O serviço deve abranger a resolução de problemas que afetem qualquer componente da solução implantada no CONTRATANTE, incluindo: revisão e ajustes em quaisquer configurações, políticas, grupos, etc; execução de instalações e atualizações; aplicação e implantação de patches, correções, updates, fixes, service packs, upgrades, builds, novas funcionalidades, novos módulos; adequações diversas; e esclarecimento de dúvidas.

1.3. DEFINIÇÕES E ESCOPOS DE SERVIÇO: Para fins de clareza e uniformidade de interpretação, estabelecem-se as seguintes definições:

1.3.1. Serviço de Suporte Técnico Especializado: Conjunto de atividades técnicas de caráter reativo, preventivo e proativo, prestadas pela CONTRATADA ou por parceiros autorizados pelo fabricante, destinado a garantir a operacionalização contínua da solução ESET Protect Enterprise On-Prem, incluindo:

1.3.1.1. Suporte Reativo: atendimento a chamados abertos pelo CONTRATANTE, com resposta e resolução conforme prazos estabelecidos no item 1.6 deste ANEXO;

1.3.1.2. Suporte Proativo: monitoramento contínuo da solução, análise de logs, identificação de vulnerabilidades, recomendações de otimização;

1.3.1.3. Manutenção Corretiva: correção de falhas, bugs, inconsistências funcionais na solução;

1.3.1.4. Manutenção Preventiva: fornecimento de atualizações de segurança, patches, releases de versão, bases de definição de vírus;

1.3.1.5. Health Checks: avaliações periódicas (trimestrais) do status da plataforma, incluindo análise de configurações, integração com ambiente, recomendações práticas de otimização;

1.3.1.6. Relatórios Estruturados: entrega de relatórios mensais detalhando atividades, indicadores, problemas identificados e ações tomadas, conforme item 11.1 deste Termo.

1.4. O serviço de suporte técnico especializado deve ser prestado em **regime 8x5, de segunda a sexta-feira, entre 09h00 e 18h00**, mediante abertura de chamado pelo CONTRATANTE por meio de chat, e-mail ou site de *helpdesk*.

1.4.1. O serviço de suporte técnico especializado deve fornecer um identificador para cada chamado aberto, acompanhando o nome do responsável e classificação do chamado, conforme previsto no contrato;

1.5. O serviço de suporte técnico especializado deve permitir também, durante toda vigência do contrato, acionamento de suporte técnico diretamente com o fabricante ESET.

1.5.1. O suporte técnico do fabricante deve ser prestado, no mínimo, em regime 8x5, de segunda a sexta-feira, entre 09h00 e 18h00, devendo obrigatoriamente ser acionado nos casos de extrapolação dos tempos de resposta máximos (item 1.6).

1.5.2. Todos os chamados abertos com o fabricante deverão ser informados ao CONTRATANTE, que deverá possuir visibilidade dos status e ações intermediadas, além de possibilidade de acompanhamento por meios dos canais oficiais de comunicação e suporte do fabricante.

1.5.3. O serviço de suporte técnico especializado deve compreender:

1.5.3.1. Designação de técnico especializado para atendimento prioritário e gestão do serviço.

1.5.3.2. Serviço de instalação e configuração com profissionais certificados ESET;

1.5.3.3. Abertura de chamados ilimitados dentro do serviço;

1.5.3.4. Acesso a laboratório de análise e detecção de malware quando o caso assim o justificar;

1.5.3.5. Acesso prioritário às equipes de desenvolvimento quando o caso assim o justificar;

1.5.3.6. Atualizações e melhorias nas versões do produto ao longo do serviço; e

1.5.3.7. Revisões periódicas do status da plataforma de segurança (*Health Checks*), garantindo um exame da integração do produto com o ambiente, análise das configurações e definições do produto e um relatório completo com conselhos práticos, incluindo sugestões para otimizar a configuração dos produtos de segurança adquiridos.

1.6. Todos os chamados abertos devem ser classificados conforme a severidade e tempo de resposta, de acordo com as definições da tabela a seguir:

SEVERIDADE	DESCRIÇÃO	PRAZO MÁXIMO PARA INÍCIO	PRAZO MÁXIMO PARA FIM
Crítico	Solução indisponível. Falha em qualquer componente da solução que impacte no correto funcionamento ou na disponibilidade da solução em produção. Falha na solução que afete serviços em produção no ambiente do CONTRATANTE. Impacto a múltiplos usuários.	30 min	8 horas
Grave	Solução parcialmente indisponível ou com degradação de tempo de resposta no acesso/uso. Falha intermitente em serviços suportados que torne o ambiente inoperante. Impacto individual ou a pequenos grupos. Operação normal afetada, mas sem interrupção..	4 horas	24 horas
Comum	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.	12 horas	72 horas

1.6.1. Entende-se como início do atendimento a proposição de solução ou medida de contorno; pedido de dados adicionais; ou a confirmação do trabalho.

1.6.2. 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.

1.6.3. Os prazos serão contados somente nos horários de atendimento do serviço.

1.6.4. O prazo de término de um atendimento será considerado como data de fechamento somente após aprovação/aceite do CONTRATANTE.

1.6.5. O descumprimento injustificado dos tempos de resposta sujeitará a contratada a glosas mensais, limitadas ao teto de 10% do valor da fatura.

1.7. Toda e qualquer ação realizada no ambiente do CONTRATANTE só poderá ser realizada com anuência e autorização do CONTRATANTE e por meio de acompanhamento de representante indicado para tal fim.

1.8. A contratada deverá disponibilizar equipe técnica composta por, no mínimo:

1.8.1. 01 profissional com Certificação ESET como *Especialista em Segurança Gerida de Clientes*;

1.8.2. 01 profissional com Certificação ESET como *Especialista de Otimização de ESET Inspect*.

1.9. Os requisitos de certificação determinados nos itens 1.7.1 e 1.7.2 devem ser comprovados durante todo o período do contrato, podendo o CONTRATANTE solicitar as devidas comprovações a qualquer momento do contrato. A comprovação deverá ser feita por meio de certificados válidos emitidos por entidades acreditadas. A exigência visa garantir a conformidade com padrões de segurança internos, considerando a natureza crítica do serviço a ser prestado.

1.10. O responsável técnico do fabricante ESET deverá fornecer relatório mensal de todos os chamados abertos no período, contendo, para cada chamado aberto: a data e hora de abertura, classificação de severidade, descrição do problema abordado e das ações realizadas, e data do fechamento do chamado (caso tenha sido fechado no período).

ANEXO II

PLANO DE SUSTENTAÇÃO E TRANSIÇÃO CONTRATUAL DE CONTRATAÇÃO DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

1. RECURSOS MATERIAIS E HUMANOS NECESSÁRIOS AO OBJETO CONTRATADO

1.1. Recursos Materiais

1.1.1. Não se aplica.

1.2. Recursos Humanos

1.2.1. Recurso humano 1:

1.2.1.1. Função: Integrante técnico

1.2.1.2. Responsável: Supervisor da SESEI

1.2.1.3. Atribuições: Analisar e definir as especificações técnicas do objeto/serviço a ser contratado; colaborar na elaboração dos artefatos do planejamento; avaliar as propostas das contratadas por ocasião da licitação; viabilizar os acessos e meios necessários para implantação dos serviços.

1.2.1.4. Quantidades/competências: 2

1.2.2. Recurso humano 2:

1.2.2.1. Função: Integrante demandante

1.2.2.2. Responsável: Diretor da Divisão de Tecnologia - DITEC.

1.2.2.3 Atribuições: Especificar os requisitos técnicos; colaborar na elaboração dos artefatos do planejamento; acompanhar o processo de contratação; avaliar as propostas das contratadas por ocasião da licitação; viabilizar os acessos e meios necessários para implantação dos serviços.

1.2.2.4. Quantidades/competências: 1

2. CONTINUIDADE DO FORNECIMENTO DA SOLUÇÃO DE TI

2.1. A continuidade dos serviços por eventual descontinuidade contratual será garantida por servidores do TRF1, o que poderá comprometer outras atividades e reduzir a qualidade do suporte, devido à limitada especialização na plataforma.

2.2. Antes de findar a vigência contratual do licenciamento atual será autuado novo processo administrativo com vistas à contratação, por ampla concorrência, de solução antivírus para a JF1.

3. ATIVIDADES DE TRANSIÇÃO CONTRATUAL E DE ENCERRAMENTO DO CONTRATO

3.1. Ações para a transição contratual

3.1.1. Não se vislumbra para esta contratação a hipótese de transição contratual.

4. ESTRATÉGIA DE INDEPENDÊNCIA

4.1. **Transferência de conhecimento:** Transferir conhecimento à equipe de TI do Contratante, para que esta possa compreender as particularidades técnicas da plataforma e prestar assessoramento aos usuários finais.

4.1.1. Descrição do item a ser transferido

Item 1: Conhecimento

4.1.1.1. Forma de transferência do Conhecimento: A equipe técnica do tribunal irá gerenciar a contratação e execução das ferramentas contratadas, com auxílio da CONTRATADA. Durante os trabalhos, dúvidas devem ser sanadas pela CONTRATADA.

4.2. Direitos de propriedade intelectual

4.2.1. Cláusulas (nos termos do artigo 93, da Lei n. 14.133/2021, concomitante com o art. 4º, da Lei n. 9.609/1998):

4.2.1.1. Toda documentação gerada na base de conhecimento será de uso exclusivo do contratante, devendo ser mantida quando do encerramento do contrato. A transferência ou repasse para a própria contratada não alocada ou terceiros só será admitida após autorização do gestor do contrato.

4.2.1.2. Como documentação gerada, entende-se por quaisquer resultados de estudos, análises, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos dos programas em qualquer mídia, páginas na Intranet e Internet e qualquer outra documentação produzida no escopo da presente contratação, em papel ou em mídia eletrônica.

4.2.1.3. A CONTRATADA deverá ceder os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados, à Administração.



Documento assinado eletronicamente por **Isabelle Cecilia de Andrade, Analista Judiciário**, em 16/06/2026, às 17:44 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Marina Alves Ferreira, Técnico Judiciário**, em 16/06/2026, às 17:58 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Juarez de Oliveira, Analista Judiciário**, em 16/06/2026, às 18:00 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Luiz Alberto Lima da Costa, Diretor(a) de Coordenadoria**, em 18/06/2026, às 14:21 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Cristina Kelly Fritsch, Técnico Judiciário**, em 25/06/2026, às 14:52 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site
<https://sei.trf1.jus.br/autenticidade> informando o código verificador **25324351** e o código
CRC **BA12592D**.

SAU/SUL - Quadra 2, Bloco A, Praça dos Tribunais Superiores - CEP 70070-900 - Brasília - DF - www.trf1.jus.br
0004467-39.2025.4.01.8000 25324351v14