PODER JUDICIÁRIO
JUSTIÇA FEDERAL

TRIBUNAL REGIONAL FEDERAL DA 2ª REGIÃO

MCTI - TERMO DE REFERÊNCIA TRF2 0999365

1. DEFINIÇÃO DO OBJETO

1.1. Contratação emergencial para aquisição de licenças de software antivírus do tipo EDR (Endpoint Detection and Response), gerenciadas por meio de plataforma unificada, para atendimento às estações de trabalho e equipamentos servidores do TRF2 e SJRJ.

1.2. Por compor uma solução única de segurança, o objeto desta contratação será indivisível.

2. DO MODELO DE PLANILHA DE FORMAÇÃO DE PREÇOS DISCRIMINADOS

2.1. A proponente deverá apresentar proposta de preços conforme modelo constante a seguir, contendo discriminação detalhada dos produtos ofertados contendo valor unitário e total, em moeda nacional brasileira, em algarismo e por extenso;

2.1.1. Como parte integrante da proposta a proponente deverá apresentar Comprovação Ponto a Ponto descrita no Anexo II deste Termo de Referência;

2.2. Na cotação de preços deverão estar inclusos todos os itens de custo e despe **s**as, tais como materiais, serviços, transportes, embalagens, seguro, mão-de-obra, salários dos profissionais, impostos, encargos sociais, encargos tributários, taxas, fretes e as demais despesas que incidam direta ou indiretamente sobre os produtos, mesmo que não estejam relacionadas na proposta.

Item	Descrição	Quantidades		Quantidade Total	Valor Unitário (R$)	Valor Total (R$)
		TRF2	SJRJ			

2.2.1	Software antivírus do tipo Endpoint Detection and Response, gerenciado por meio de uma plataforma unificada para atendimento às estações de trabalho e equipamentos servidores do TRF2 e SJRJ, com suporte e atualizações por 3 (três) meses. Código SIASG 350949	2.000	4.000	6.000		
2.2.2	Software antivírus para Microsoft Exchange Código SIASG 350947	3.700	8.000	11.700		
					Valor Total	

3. DA DESCRIÇÃO DA SOLUÇÃO DE TIC

3.1. A solução de segurança do tipo EDR (Endpoint Detection and Response) deve ser composta por uma plataforma centralizada de administração. Todos os itens componentes desta solução devem ser fornecidos pelo mesmo fabricante, viabilizando a perfeita integração entre as diversas camadas do sistema.

4. DA JUSTIFICATIVA E MOTIVAÇÃO DA CONTRATAÇÃO

4.1. A aquisição tem por objetivo garantir a continuidade do negócio, através da aquisição de solução existente de segurança do tipo *Endpoint Detection and Response*, utilizando uma plataforma unificada de gerenciamento por localidade e visando a proteção das estações de trabalho e equipamentos servidores do TRF2 e SJRJ.

4.2. Com essa aquisição garante-se o direito às atualizações de software e dos mecanismos de proteção necessários para o correto funcionamento da solução de segurança, bem como suporte técnico junto ao fornecedor/fabricante para solução de problemas mais complexos que possam ocorrer.

4.3. Essa solução possui, em verdade, uma atuação muito mais abrangente na segurança do ambiente de tecnologia da informação corporativa, combinando ferramentas de proteção contra outras ameaças digitais, sendo indispensável a qualquer corporação nos dias atuais.

4.4. Pelo exposto, essa contratação é imprescindível para a manutenção dos padrões atuais de segurança de TI,

essencial para o correto funcionamento da rede de computadores corporativa do órgão.

5. DOS RESULTADOS / BENEFÍCIOS A SEREM ALCANÇADOS

5.1. Garantir a segurança dos usuários ao abrir arquivos de dados.

5.2. Garantir a segurança da Rede Corporativa.

5.3. Garantir a segurança dos computadores da instituição.

6. DO ALINHAMENTO DA CONTRATAÇÃO E O PLANEJAMENTO ESTRATÉGICO DA JF

6.1. Esta contratação enquadra-se nos seguintes objetivos constantes do Plano Estratégico de TI da Justiça Federal (PETI-JF) 2021-2026, constantes da Resolução CJF nº 685/2020:

6.1.1. Aperfeiçoar e Assegurar efetividade dos serviços de TI para a Justiça Federal.

6.2. Esta contratação enquadra-se no seguinte objetivo estratégico do ENTIC-JUD constante da Resolução nº 370/2021 do CNJ alterada pela Resolução nº 396/2021:

6.2.1. Aprimorar a Segurança da Informação e a Gestão de Dados.

6.3. Esta contratação está alinhada ao seguinte item do art. 1º da Resolução 396/2021 do CNJ, que trata da Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ):

6.3.1. Ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade das atividades-fim e administrativas dos órgãos do Poder Judiciário.

6.4. Esta contratação enquadra-se nas seguintes iniciativas/necessidades descritas no PDTI 2024-2026 da Justiça Federal da 2ª Região:

6.4.1. Continuidade e disponibilidade da infraestrutura de TI;

6.4.2. Segurança da Informação no âmbito da TI.

7. DA REFERÊNCIA AOS ESTUDOS PRELIMINARES DA CONTRATAÇÃO

7.1. Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) SEI DOD TRF2 0993792 e os Estudos Preliminares (artefatos) constantes no Processo SEI 0010031-69.2025.4.02.8000.

8. DA RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE BENS E/OU SERVIÇOS A SEREM CONTRATADOS

8.1. A relação entre a demanda prevista e a quantidade de bens e/ou serviços a serem contratados considerou as licenças já existentes e em uso no TRF2 e SJRJ.

8.2. O quantitativo de licenças abrange o atendimento das seguintes demandas:

8.2.1. Até 2.000 licenças para assegurar a segurança de equipamentos do TRF2;

8.2.2. Até 4.000 licenças para assegurar a segurança de equipamentos da SJRJ;

8.2.3. Até 3.700 licenças para assegurar a segurança de caixas de e-mail do TRF2;

8.2.4. Até 8.000 licenças para assegurar a segurança de caixas de e-mail da SJRJ;

9. DO LEVANTAMENTO DAS ALTERNATIVAS E ANÁLISE DE MERCADO DE TIC

9.1. Ao realizar a análise do mercado de TI foram encontradas as seguintes alternativas:

9.1.1. Renovação do licenciamento da solução de segurança existente;

9.1.2. Adoção de uma solução de segurança baseada em software livre;

9.1.3. Aquisição completa de uma nova solução de segurança.

9.2. A primeira alternativa é a que menos gera esforço, tendo em vista que não implica em substituir os

softwares e configurações existentes. Como trata-se de uma contratação emergencial pelo período de 03 (três) meses é a que mais se adapta a necessidade premente de aquisição. A contratação é do tipo EDR (Endpoint Detection and Response) que detecta ameaças conhecidas e desconhecidas, incluindo ameaças persistente avançadas (APTs) por meio de análise comportamental e detecção de anomalias. Esta contratação é a solução mais básica do fabricante Kaspersky. Esta foi a alternativa escolhida.

9.3 A segunda alternativa tendo em vista a dimensão da contratação do antivírus para a Justiça Federal da Segunda Região, que necessita de 8.400 licenças de antivírus com ferramenta EDR integrada numa estrutura hierarquizada, foi feito o levantamento de ferramentas "Open Source" e de ferramentas proprietárias tomando como base o quadrante mágico do Gartner e o 'The Forrester Wave for Endpoint Detection and Response do 2° Quadrante de 2022' da Forrester. Dentre as ferramentas open source, não foram encontradas soluções que garantissem a segurança, proteção e pronta resposta, visto que essa categoria de software é mantida e atualizada por uma comunidade aberta, sem órgãos ou entidades que assegurem o suporte técnico adequado. Funcionalidades como integração de EPP e EDR, detecção de ameaças em tempo real, análise de comportamento proativa, atualizações e correções com rápido tempo de resposta, são aspectos limitantes nos softwares open source, quando comparados as soluções proprietárias, o que inviabiliza a adoção de ferramentas livres para atender uma estrutura de TI complexa e de alta criticidade como a da Justiça Federal da Segunda Região. Também se levou em conta a carência de profissionais capacitados em prestar o devido suporte técnico especializado em ferramentas open source e a baixa disponibilidade de empresas para assessorar a implantação, monitoramento, atualização e proposição de melhorias em tempo hábil de pronta resposta que as ferramentas EDR exigem, além do SLA (Acordo de Nível de Serviço) ser muito longo, pois depende, em sua maioria, de apoio e resposta de comunidades de desenvolvedores.

9.4 A terceira e última alternativa que consiste em adquirir uma nova solução completa de segurança. Face a termos que ter os custos de treinamento na nova solução e por se tratar de uma contratação emergencial enquanto a licitação definitiva não sai, ela se torna pouco atrativa.

10. DA JUSTIFICATIVA DA ALTERNATIVA ESCOLHIDA

10.1. A opção pela **primeira** alternativa tem por base a vantajosidade elencada no item **9.2**.

11. DA NATUREZA DO OBJETO

11.1. A natureza do objeto foi analisada segundo os critérios descritos na tabela abaixo:

Critério	Atendimento da solução
É possível especificar o serviço usando parâmetros usuais de mercado?	Sim
É possível medir o desempenho da qualidade usando parâmetros usuais de mercado?	Sim
O objeto da contratação se estende necessariamente por mais de um ano?	Sim
O objeto da contratação é essencial para o negócio?	Sim

12. DO PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

12.1. Os itens da contratação possuem relação de interdependência, pois, compõem licenciamento e suporte especializado de uma única solução, perfazendo o direito sobre um único produto/fabricante. Assim sendo, a

divisão dos itens com adjudicação a empresas distintas comprometerá o atendimento das necessidades do Contratante, devendo ser o objeto da Licitação uno e indivisível.

13. DA MODALIDADE E TIPO DE LICITAÇÃO

13.1. Verifica-se que o objeto da contratação pretendida é oferecido por diversas revendas do fornecedor atual e apresenta características padronizadas e usuais. Por tratar-se de uma contratação emergencial pelo período de 3 (três) meses, a melhor opção a utilização da contratação direta por dispensa de licitação após a devida pesquisa de preços de mercado.

14. DO IMPACTO AMBIENTAL DECORRENTE DA CONTRATAÇÃO

14.1. A CONTRATADA deverá respeitar e cumprir todas as disposições da legislação ambiental vigente, responsabilizando-se perante o CONTRATANTE, os Órgãos Ambientais e terceiros, por todo e qualquer dano ou prejuízo que porventura cause ao Meio Ambiente.

14.2. Com o licenciamento por subscrição, entende-se que não serão fornecidos quaisquer tipos de mídias, nem material que exijam embalagens e transporte. Com essa ação, o CONTRATANTE atua em prol da sustentabilidade visando uma economia de baixo carbono.

15. DA CONFORMIDADE TÉCNICA E LEGAL

15.1. Resolução TRF2-RSP-2023/00043 que trata sobre a Política de Segurança da Informação da Justiça Federal da 2ª Região.

16. DOS CRITÉRIOS DE HABILITAÇÃO TÉCNICA

16.1. Para fins de habilitação, deverá ser apresentado atestado de capacidade técnica emitido por instituição ou empresa de direito público ou privado no Brasil, impresso em papel timbrado (não serão aceitas declarações genéricas de catálogos, manuais ou Internet), contendo nome e telefone de contato dos responsáveis pela informação atestada, comprovando o fornecimento de objeto compatível similar ao especificado neste Termo de Referência;

16.2. Considera-se que o objeto é similar caso seja de fornecimento de solução de segurança contendo licenças de antivírus tipo EDR em quantitativo de pelo menos 50% ao ofertado neste Termo de Referência, sendo válida a apresentação de mais de um documento para a comprovação do quantitativo exigido, além de serviços de instalação, suporte técnico e garantia;

16.3. O documento deverá ainda atestar a satisfação da instituição ou empresa de direito público ou privado no Brasil com os produtos ofertados pela proponente;

16.4. Não serão aceitos atestados emitidos pela própria proponente ou por suas revendas ou distribuidores;

16.5. A exigência visando à comprovação da capacidade técnica da proponente, limitada aos critérios técnicos preponderantes e de maior relevância do objeto, se justifica em função da complexidade inerente à configuração da solução de segurança ora contratada. Releva-se igualmente o fato de tratar-se de solução voltada à segurança da informação e à disponibilidade do negócio, tornando, portanto, inadequada a prestação de serviços de implantação por parte de empresas que não possuem a devida qualificação técnica mínima.

17. DOS REQUISITOS DA CONTRATAÇÃO

17.1. Especificações técnicas mínimas – **item 2.2.1**

17.1.1. A CONTRATADA deverá fornecer licenças de software antivírus do tipo Endpoint Detection and Response, ora denominada como SOLUÇÃO, com suporte para atualizações de no mínimo 3 (três) meses contados da data da emissão do termo de recebimento definitivo, atendendo aos requisitos técnicos descritos e abrangendo as exigências a seguir:

17.1.2. <u>DAS CARACTERÍSTICAS DAS LICENÇAS</u>

17.1.2.1. O serviço de atualização das licenças será prestado dentro do período de suporte e

consiste na disponibilização via Internet para o CONTRATANTE de todas as versões (upgrades), atualizações (releases) e correções (updates), de forma a manter a solução permanentemente atualizada, bem como, no fornecimento de manuais e boletins técnicos com informações que assegurem a plena utilização dos produtos licenciados sem custo adicional para o CONTRATANTE;

17.1.2.2. Os serviços de proteção e de atualização das assinaturas e mecanismos de segurança deverão funcionar em regime 24x7x365.

17.1.3. DOS ASPECTOS GERAIS DA SOLUÇÃO

17.1.3.1. A SOLUÇÃO ofertada deverá ser de uma única empresa desenvolvedora de software de modo que tanto o suporte à SOLUÇÃO quanto as funcionalidades sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento;

17.1.3.1.1. Excepcionalmente, será admitido que a SOLUÇÃO tenha plataforma de gerenciamento em separado para o Microsoft Exchange desde que seja da mesma empresa desenvolvedora da SOLUÇÃO.

17.1.3.2. Os servidores de gerenciamento da SOLUÇÃO deverão possibilitar a distribuição de carga e administração em níveis hierárquicos (primário e secundário), em grupos lógicos independentes da estrutura de domínio de rede, de acordo com regiões geográficas, departamentos etc.;

17.1.3.3. Deverá suportar comunicação cliente/servidor através dos protocolos de rede TCP/IP;

17.1.3.4. Deverá fornecer proteção e remoção integrada, através de um única SOLUÇÃO, contra vírus, trojans, worms de rede, spywares, adwares e rootkits, bem como incorporar funcionalidades de firewall pessoal e IPS (intrusion Prevention System);

17.1.3.5. Deverá fornecer proteção de ameaças da Web através de serviço de reputação de site;

17.1.3.6. Será admitida a implementação desse recurso mediante plugin para o navegador WEB;

17.1.3.7. Possibilidade de efetuar backup da base de dados da solução;

17.1.3.8. Possuir solução de File Reputation (reputação de arquivos), integrada e gerenciada através da console do antivírus, cancelando o download ou execução do arquivo, de forma automática caso o mesmo tenha conteúdo malicioso, baseado na resposta à consulta da base da empresa desenvolvedora da SOLUÇÃO;

17.1.3.9. Possibilidade de configuração de bloqueio de acesso aos sites maliciosos pela console de gerenciamento;

17.1.3.9.1. Será admitida a implementação desse recurso via atuação manual ou de forma automática.

17.1.3.10. Possibilidade de criar blacklists e whitelists de URLs para estações pela console de gerenciamento;

17.1.3.10.1. Será admitida a implementação desse recurso via atuação manual ou de forma automática.

17.1.3.11. Deverá realizar scanner de ameaças do tipo completa (full);

17.1.3.12. Deverá ser fornecida no idioma Inglês-US e português do Brasil;

17.1.3.13. Na medida em que novas versões (upgrades), ou correções pontuais (updates) de problemas (bugs) forem introduzidas pela empresa desenvolvedora de software, a CONTRATADA deverá disponibilizar cópias dessas atualizações (upgrades ou updates) para que elas sejam incorporadas no ambiente do CONTRATANTE;

17.1.3.14. A CONTRATADA deverá fornecer informações sobre como o CONTRATANTE terá acesso ao serviço de suporte técnico para abertura de chamado e sobre como obter atualizações da SOLUÇÃO.

17.1.4. DA INSTALAÇÃO E ADMINISTRAÇÃO DA SOLUÇÃO

17.1.4.1. Deverá prover mecanismos de instalação em clientes e servidores *Windows* através de *login script* com instalação remota a partir da console ou através da rede.

17.1.4.2. Deverá prover mecanismos de customização dos pacotes de instalação em clientes e servidores, provendo ainda funcionalidades avançadas de customização como:

17.1.4.2.1. Instalação silenciosa.

17.1.4.2.2. Pastas de instalação no destino.

17.1.4.2.3. Configurações avançadas das tecnologias a serem instaladas.

17.1.4.3. Os pacotes deverão ser otimizados para instalação em cada uma das plataformas existentes no ambiente de TIC do CONTRATANTE, conforme o caso.

17.1.4.4. O pacote deverá detectar automaticamente a versão do sistema operacional do computador destino e instalar a SOLUÇÃO correspondente sem a necessidade de intervenção do administrador ou do usuário.

17.1.4.5. A customização do pacote de instalação deverá permitir que a distribuição seja feita para os computadores em conformidade com a política de configuração determinada pelo administrador, juntamente com as últimas vacinas, em um único processo transparente e silencioso.

17.1.4.6. Deverá suportar instalações em clientes remotos e móveis (notebooks) sem depender de outro software ou agente previamente instalado.

17.1.4.7. Deverá possuir capacidade de detecção de violações na integridade da instalação ou dos arquivos do antivírus instalado nos clientes e servidores.

17.1.4.8. Deverá possuir uma ferramenta que permita analisar toda a rede e identificar os computadores que porventura não estejam com o antivírus instalado ou atualizado, de acordo com as políticas determinadas na console de administração.

17.1.4.9. A solução deverá ser capaz de identificar solução de terceiros que esteja instalada no host e realizar a remoção desta no momento da instalação da solução CONTRATADA.

17.1.4.10. Deverá apresentar administração centralizada de todos os clientes e servidores Windows em console única de gerenciamento baseado na tecnologia MMC (Microsoft Management Console) ou através de interface WEB.

17.1.4.11. O console único de gerenciamento deve exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, versão do antivírus, versão dos mecanismos de verificação (engine), data da vacina, data da última verificação e endereço IP.

17.1.4.12. O console único de gerenciamento deverá permitir travamento das configurações em clientes e servidores para que somente o administrador possa alterar a configuração, desinstalar ou parar a SOLUÇÃO.

17.1.4.13. O console único de gerenciamento deve permitir a proteção de acesso aos servidores de administração do sistema e grupos lógicos de computadores, através de senhas configuradas pelo administrador.

17.1.4.14. O console único de gerenciamento deve exibir logs e alertas de todos os clientes e servidores, em tempo real, sem a necessidade de exportar ou transferir arquivos manualmente ou através de batches entre clientes, servidores e central de gerenciamento.

17.1.4.15. Possuir capacidade de aplicar mudanças na configuração do antivírus em clientes e servidores Windows, com possibilidade de mudança para todos os computadores, para um determinado grupo de computadores ou para um único computador.

17.1.4.16. As configurações da SOLUÇÃO em clientes e servidores, após modificadas na central de administração, deverão ser distribuídas para os computadores, automaticamente, sem a necessidade de uso de agentes externos, *login scripts*, tarefas manuais ou outros módulos adicionais.

17.1.4.17. As novas configurações deverão ser efetivamente instaladas e ativadas no computador destino sem a necessidade de reinicialização ou *logoff / logon* do usuário.

17.1.4.18. Deverá possuir capacidade de envio de alertas, no caso de mudanças de configuração, ativação ou desativação do antivírus, atualização de vacinas e incidência de vírus.

17.1.4.19. O console de gerenciamento deverá ter a capacidade de abrir uma única janela de alerta de vírus com todas as ocorrências, com o intuito de se evitar a exibição de uma nova janela para cada alerta gerado.

17.1.4.20. A instalação deverá ser possível sem necessidade de reiniciar a estação de trabalho.

17.1.4.21. Deverá ser possível gerar imagens (modelos padronizados para instalação) de estações de trabalho com a SOLUÇÃO.

17.1.4.22. Deverá possibilitar o agrupamento de máquinas em grupos, com configurações específicas para cada grupo criado.

17.1.4.23. Deverá realizar a autorreparação de danos causados por *Trojan Horses*, de forma

automática, sem necessidade de agentes ou pacotes adicionais. Essa função deverá ser nativa da SOLUÇÃO e automática, dispensando a intervenção do administrador.

17.1.4.24. Deverá possuir a capacidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado.

17.1.4.25. Permitir a utilização de fontes de agentes de atualização secundários em localidades remotas com objetivo de minimizar o consumo do *link* durante a atualização de vacinas; Estes agentes devem ser configurados através da própria console de gerenciamento sem a necessidade de intervenção local ou instalação de outro *software*.

17.1.4.26. Deverá permitir a varredura dos dispositivos removíveis e periféricos (pen drives, *USB, memórias flash, etc.,*) mesmo com a política de bloqueio total ativa.

17.1.4.27. O console único de gerenciamento deverá permitir a criação de usuários com diferentes níveis de administração.

17.1.4.28. O console único de gerenciamento deverá permitir integração com o *Active Directory* para identificar máquinas presentes no AD e que não tenham a ferramenta de antivírus instalada, possibilitando ainda a instalação automática da ferramenta para garantir a integridade da rede.

17.1.4.29. Proteção contra desinstalação e desativação não autorizada da SOLUÇÃO.

17.1.4.30. Permitir a instalação em ambientes em *Cluster Microsoft*.

17.1.4.31. Configuração de *Dashboard* com medição do nível de atualização do ambiente ou do nível de cumprimento de política de segurança previamente definida.

17.1.5. DAS ATUALIZAÇÕES DE VACINAS E CORREÇÕES DA SOLUÇÃO

17.1.5.1. Capacidade de atualizar remotamente e em tempo real a vacina e engine da SOLUÇÃO, em um único pacote para todas as plataformas suportadas, sem a necessidade de utilização de login scripts, agendamentos nas estações ou intervenção do usuário e sem requerer reinicialização do computador ou do serviço Antivírus para aplicação das atualizações.

17.1.5.2. As atualizações deverão ser feitas a partir de comunicações agendadas ou manuais, entre o servidor de administração e o centro de pesquisas da empresa desenvolvedora da SOLUÇÃO, com mecanismos de checagem de autenticidade e com periodicidade mínima semanal.

17.1.5.3. Deverá prover mecanismos de distribuição de vacinas para toda a rede a partir de servidor de administração, de forma agendada e real-time, e com pacotes incrementais, de forma a prevenir a alta utilização de banda de rede.

17.1.5.4. Deverá ter mecanismos de configuração para o agendamento do envio de vacinas, com tolerância a falhas, para que a tarefa de atualização seja executada dentro de um período determinado, após o horário pré-agendado, e com o intuito de garantir a atualização de clientes e servidores que estivessem anteriormente indisponíveis (desligados, em processo de reinicialização, etc.).

17.1.5.5. A tarefa de atualização das vacinas deverá possuir mecanismos de randomização, baseados em dias da semana, minutos ou dias, após o horário pré- agendado da atualização, diminuindo assim o tráfego de rede gerado pela SOLUÇÃO no processo de atualização.

17.1.5.6. O processo de atualização deverá prover mecanismos de configuração para que os clientes façam a busca por novas vacinas, nos servidores de antivírus, em intervalos periódicos e em escala de minutos.

17.1.5.7. Capacidade de executar a volta imediata para a vacina anterior, através da console de gerenciamento, de forma silenciosa e sem intervenção do usuário, para o caso de a vacina atual apresentar problemas.

17.1.6. DOS MECANISMOS DE VERIFICAÇÃO DA SOLUÇÃO

17.1.6.1. Compatível com plataformas existentes no ambiente de TIC do CONTRATANTE:

17.1.6.2. Rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados, incluindo sessões *DOS* abertas pelo *Windows*, bem como servidores *Linux*.

17.1.6.3. Rastreamento manual com interface *Windows*, customizável, com opção de limpeza.

17.1.6.4. Capacidade de detecção de vírus desconhecidos da vacina mais atual, inclusive de macros do *MS Office*, utilizando análise heurística, análise comportamental ou aprendizado de máquina (*machine learning*).

17.1.6.5. Detecção de programas maliciosos como *spyware*, programas de propaganda, ferramentas como *password crackers*, dentre outros.

17.1.6.6. Detecção e reparo de arquivos contaminados, mesmo compactados por ZIP, CAB e ARJ.

17.1.6.7. Permitir configurar ações a serem tomadas na ocorrência de vírus, incluindo, dentre outras, reparar, deletar, mover para a área de Isolamento (quarentena) e ignorar.

17.1.6.8. Possibilidade de quarentenar o arquivo suspeito antes de limpá-lo.

17.1.6.9. Rastreamento remoto, de modo manual ou agendado.

17.1.6.10. Possuir mecanismos de área de isolamento de arquivos para vírus desconhecidos ou sem possibilidade de reparação (área de quarentena).

17.1.6.11. A área de isolamento deverá remover o arquivo infectado do computador de origem da suspeita de infecção.

17.1.6.12. Deverá existir a possibilidade de envio de amostras para o centro de pesquisas da empresa desenvolvedora da SOLUÇÃO.

17.1.6.13. A resposta da empresa desenvolvedora da SOLUÇÃO deverá prover vacina para a amostra enviada que deverá ser adicionada às vacinas existentes, além de tentar reparar os arquivos isolados na área de quarentena.

17.1.6.14. A área de isolamento deverá possibilitar a devolução dos arquivos livres de vírus que tenham sido colocados em quarentena para seus pontos de origem.

17.1.6.15. Capacidade para, em caso de epidemia, bloquear acesso a pastas compartilhadas, a portas TCP e UDP, e escrita em diretórios e arquivos específicos, restaurando as configurações originais ao término da epidemia de forma automática através de políticas recebidas da empresa desenvolvedora da SOLUÇÃO ou de forma manual pela console de gerenciamento.

17.1.6.16. Possibilidade de colocar arquivos e diretórios em listas de exclusões para não serem verificados pelo antivírus.

17.1.6.17. Possibilidade de bloquear aplicações com base no nome, diretório ou extensão do arquivo ou também com base no *hash* da aplicação.

17.1.6.18. Possibilidade de proteger o computador permitindo que somente determinadas aplicações (com base no *hash*) possam ser executadas.

17.1.6.19. Notificação automática ao administrador em caso de epidemia de vírus.

17.1.6.20. *Firewall* com capacidade de verificação dos pacotes que estão entrando e/ou saindo da estação de trabalho, com detecção e bloqueio de ataques de *malwares* que exploram vulnerabilidades em *software*.

17.1.6.21. Capacidade de detecção de ameaças que utilizam algoritmos de compactação em tempo real não padronizados com objetivo de não serem identificados.

17.1.6.22. Permitir o reinício automático dos serviços do antivírus caso esse tenha sido parado devido a algum código malicioso, sem a necessidade da intervenção do administrador.

17.1.6.23. Permitir autoproteção ao cliente de antivírus em nível de registro, arquivos de programa e processos.

17.1.6.24. Capacidade de identificar a origem (servidores ou estações) de ataques de *malwares* na rede local.

17.1.7. <u>ENDPOINT DETECTION AND RESPONSE</u>

17.1.7.1. Permitir o envio de dados de telemetria para a console continuamente.

17.1.7.2. Permitir o envio de dados de telemetria a partir da criação e edição de arquivo independentemente do tipo de extensão.

17.1.7.3. Apresentar todas as informações relevantes de um incidente na tela de detalhes do alerta, com, pelo menos, as seguintes informações: Usuários, Ativos, Domínios, IPs, Hashes, Processos ou Técnicas/Táticas identificadas.

17.1.7.4. Identificar se um processo em execução é seguro ou não por, pelo menos, um dos

seguintes métodos: Sistema de reputação do fabricante, Análise de comportamento ou Regras de indicadores.

17.1.7.5. Permitir a geração de alertas a partir de alertas de detecção de comportamento (Behavior Detection) baseado em dados de telemetria obtidos de agente e tráfego de rede do endpoint.

17.1.7.6. Proteger contra técnicas de exploração de memória.

17.1.7.7. Bloquear ataques envolvendo reverse shell.

17.1.7.8. Bloquear ataques envolvendo exploração de vulnerabilidades de Serialização/Desserialização.

17.1.7.9. Permitir a remoção de arquivos maliciosos em repouso.

17.1.7.10. Permitir a customização de consultas por meio de API, possibilitando a geração de relatórios personalizados.

17.1.7.11. Permitir a exportação de relatórios.

17.1.7.12. Deve manter cache de eventos, alertas e telemetria no endpoint mesmo após sua reinicialização, até que seja possível enviar à console de gerência.

17.1.7.13. Detectar ataques de força bruta para autenticação de endpoints.

17.1.7.14. Detectar o uso indevido de DLL's confiáveis.

17.1.7.15. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

17.1.7.15.1. Impedir a execução de objetos.

17.1.7.15.2. Isolamento de host.

17.1.7.15.3. Excluir objeto do host ou grupo de hosts.

17.1.7.15.4. Encerrar um processo no dispositivo.

17.1.7.15.5. Colocar um objeto em quarentena.

17.1.7.15.6. Execute a verificação do sistema.

17.1.7.15.7. Execução remota de programa/processo/comando.

17.1.7.15.8. Iniciar a varredura IoC para um grupo de hosts.

17.1.7.16. Todas as funcionalidades abordadas neste tópico devem ser aplicadas a sistemas operacionais Windows com suporte ainda vigente.

17.1.7.17. Os requisitos apresentados neste tópico poderão ser atendidos pela solução de antivírus fornecida sem necessidade de serem exclusivamente atendidos pelas funcionalidades e/ou módulo de EDR.

17.2. Especificações técnicas mínimas – **item 2.2.2**

7.2.1 Sofware Antivirus para MICROSOFT EXCHANGE

17.2.1.1. Instalação nas plataformas Microsoft Windows Server 2012R2 Server até a mais atual existente;

17.2.1.2. Suporte a Microsoft Exchange 2013 e todas as demais versões do Microsoft Exchange até a mais atual existente;

17.2.1.3. Rastreamento em tempo real, para arquivos anexados a mensagens do Microsoft Exchange, antes de entregar a mensagem na caixa postal do(s) destinatário(s), com as seguintes opções:

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

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

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

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

17.2.1.5. Programação de rastreamentos automáticos do Exchange com as seguintes opções:

17.2.1.5.1. Escopo: Todas as pastas locais, ou pastas específicas, unidades removíveis,

unidades de rede mapeadas, memória para rootkits, processos em execução e arquivos registrados;

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

17.2.1.5.3. Frequência: Horária, diária, semanal, mensal.

17.2.1.6. Gerar registro (log) dos eventos de vírus em arquivo com limite de tamanho opcional.

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

17.2.1.8. Identificação de remetente e destinatário das mensagens.

17.2.1.9. Permitir bloqueios baseados nos seguintes critérios:

17.2.1.9.1. Tipo de arquivo;

17.2.1.9.2. Nome do arquivo;

17.2.1.9.3. Tamanho do arquivo.

17.2.1.10. Permitir a instalação em ambientes em Cluster Microsoft.

18. DAS CONDIÇÕES E PRAZOS DE ENTREGA

18.1. Os licenciamentos terão como destino os seguimtes órgãos:

18.1.1. Tribunal Regional Federal da 2a Região: 2.000 licenças antivirus tipo EDR e 3.700 licenças para Microsoft Exchange.

18.1.2. Seção Judiciária do Rio de Janeiro: 4.000 licenças antivirus tipo EDR e 8.000 licenças para Microsoft Exchange.

18.2. As licenças deverão ser entregues por e-mail, em até 10 (dez) dias, contados a partir do primeiro dia seguinte à assinatura do contrato, da seguinte forma:

18.2.1. O e-mail terá como destinatários: agsi@trf2.jus.br com cópia para tscoocon@trf2.jus.br;

18.2.2. Na mensagem eletrônica deverão constar, além dos dados requeridos para o licenciamento no site do fabricante:

18.2.2.1. Cópia da nota fiscal;

18.2.2.2. Os procedimentos a serem adotados para ativação das licenças;

18.2.2.3. O telefone e/ou e-mail de contato para suporte ao procedimento;

18.2.2.4. A forma de comprovação junto ao site do fabricante dos itens fornecidos com suas descrições, respectivos part-numbers e quantitativos em nome do Contratante e com o prazo de vigência/garantia.

18.2.3. Caso não ocorra confirmação do recebimento de mensagens no prazo de 24 horas, a Contratada deverá entrar em contato com a equipe técnica no telefone (21) 2282-7791;

18.3. A entrega dos bens e dos serviços deverá ser realizada observando os prazos descritos no item 20 (Cronograma de Execução).

19. DO CRONOGRAMA DE EXECUÇÃO

19.1. A tabela abaixo sintetiza as etapas de execução desta contratação. O prazo em todas as etapas tem como referência inicial o fim da etapa anterior:

Etapa	Descrição	Prazo
01	Assinatura do Contrato	-
02	Entrega dos produtos (software)	Em até 10 (dez) dias após a Etapa 01

03	Recebimento provisório do objeto	Logo após a conclusão das Etapas 02
04	Recebimento definitivo do objeto	Em até 10 (dez) dias após a Etapa 03

20. DAS OBRIGAÇÕES DO CONTRATANTE

20.1. Assegurar o acesso às suas dependências dos profissionais incumbidos de prestar os serviços contratados, desde que se apresentem devidamente identificados, respeitadas as normas internas (segurança, disciplina) do Contratante;

20.2. Proporcionar condições e prestar informações à Contratada, necessários ao cumprimento do objeto do Contrato;

20.3. Comunicar à Contratada qualquer irregularidade verificada no cumprimento do objeto do Contrato, determinando, de imediato, a adoção de medidas necessárias à solução dos problemas;

20.4. Acompanhar e fiscalizar rigorosamente o cumprimento do objeto da contratação;

20.5. Manter a Contratada atualizada sobre os padrões de instalação, operação, configuração, segurança tecnológica e segurança da informação adotada no âmbito do Contratante, a fim de que seu pessoal técnico esteja sempre habilitado à execução dos serviços contratados;

20.6. Recusar o recebimento de material ou serviço que não estiver em conformidade com as especificações constantes da proposta apresentada pela Contratada ou em desacordo com as especificações técnicas do Termo de Referência.

21. DAS OBRIGAÇÕES DA CONTRATADA

21.1. Entregar e instalar todos os itens dentro dos prazos previstos. Caso a entrega e/ou a instalação dos itens não seja feita dentro dos prazos, a Contratada ficará sujeita às sanções estabelecidas no Contrato;

21.2. O Contratante não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para outras entidades, sejam fabricantes, subcontratadas, representantes ou quaisquer outros;

21.3. Responder por perdas e danos que vier a causar ao Contratante ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou de seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;

21.4. Arcar com todas as despesas com deslocamento, alimentação e estadia para realização dos serviços na sede do Contratante;

21.5. Ser responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais, resultante da execução do Contrato;

21.6. Comunicar ao Contratante, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos necessários;

21.7. Manter durante toda a execução do Contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas por lei neste Termo de Referência e na Licitação;

21.8. Manter sob seus cuidados e discrição, impedindo a divulgação, publicação ou disseminação das informações do Contratante a que tiver acesso ou conhecimento para fins de execução de suas atividades relativas ao cumprimento do Contrato;

21.9. As partes desde já ajustam que não existirá para o Contratante solidariedade quanto ao cumprimento das obrigações trabalhistas e previdenciárias para com os empregados da Contratada, cabendo a esta assumir, de forma exclusiva, todos os ônus advindos da relação empregatícia.

22. DOS PAPÉIS A SEREM DESEMPENHADOS PELOS PRINCIPAIS ATORES DO ÓRGÃO E DA EMPRESA ENVOLVIDOS NA CONTRATAÇÃO

22.1. Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao

processo de gestão do Contrato;

22.2. Fiscal Requisitante do Contrato: servidor representante da Área Requisitante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos funcionais da solução;

22.3. Fiscal Técnico do Contrato: servidor representante da Área de Segurança da Informação indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos técnicos da solução;

22.4. Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

23. DOS MECANISMOS FORMAIS DE COMUNICAÇÃO ENTRE CONTRATANTE E CONTRATADA

23.1. Sempre que se exigir, a comunicação entre o representante do Contratante e da Contratada deverá ser formal, considerando-se como documentos formais, além de documentos do tipo Ofício, as comunicações por correio eletrônico e outras especificadas no Edital e no Contrato;

23.2. Deverá ser fornecido telefone fixo isento de tarifação telefônica (por exemplo, prefixo 0800), número local do Rio de Janeiro (RJ) para o TRF2/SJRJ ou sistema de informação apropriado via Internet para abertura dos chamados.

24. DOS INSTRUMENTOS FORMAIS DE SOLICITAÇÃO DE FORNECIMENTO DOS BENS E/OU PRESTAÇÃO DE SERVIÇOS

24.1. Conforme item 23.1.

25. DOS NÍVEIS DE SERVIÇOS EXIGIDOS (NSE)

25.1. Não se aplica.

26. DA APLICAÇÃO DE GLOSAS

26.1. Não se aplica.

27. DAS CONDIÇÕES DE RECEBIMENTO PROVISÓRIO E DEFINITIVO DO OBJETO

27.1. Em conformidade com o artigo 140 da Lei n. º 14.133/2021, o objeto do Contrato será recebido da seguinte forma:

27.1.1. Provisoriamente – de forma sumária, mediante recibo aposto no documento fiscal, por responsável pelo acompanhamento e fiscalização, imediatamente depois de efetuada a entrega dos itens, material para efeito de posterior verificação;

27.1.2. Definitivamente - por servidor ou comissão designada pela autoridade competente, mediante termo detalhado, assinado pelas partes, que comprove o atendimento das exigências contratuais, no prazo de 10 (dez) dias, contados a partir do recebimento provisório, salvo motivo justificado.

27.2. O objeto do Contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com as especificações do Edital e seus anexos;

27.3. O recebimento provisório ou definitivo não exclui a obrigação da Contratada em reparar, corrigir, remover, reconstituir ou substituir às suas expensas, no total ou em parte, no prazo de 05 (cinco) dias úteis, contado da solicitação do Contratante, o objeto deste Edital, em que se verificarem vícios, defeitos ou incorreções;

27.4. O aceite/aprovação do(s) produto(s) pelo órgão licitante não exclui a responsabilidade civil do fornecedor por vícios de quantidade ou qualidade do(s) produto(s) ou disparidades com as especificações estabelecidas, verificadas, posteriormente, garantindo-se ao Contratante as faculdades previstas no artigo 18 da Lei nº 8.078/1990;

27.5. Ao receber os itens, o Contratante verificará se o quantitativo e a descrição de cada item entregue está de acordo com o quantitativo especificado na solicitação de fornecimento de bens e com a descrição constante neste Termo de Referência. Não havendo divergências, o Contratante emitirá o Termo de Recebimento Provisório;

27.6. Após a instalação e configuração dos itens pela Contratada, o Contratante, com o apoio de técnico(s) da Contratada, efetuará testes, objetivando verificar a conformidade com as especificações deste Termo de Referência, bem como aferir o perfeito funcionamento dos itens;

27.7. Concluída a fase de testes dos itens e não tendo sido verificadas anormalidades, o Contratante emitirá o Termo de Recebimento Definitivo, respeitando-se o prazo limite para a sua emissão, iniciando-se a partir dessa data a contagem dos prazos para garantia dos objetos contratados;

27.8. A(s) referida(s) Nota(s) Fiscal(is) dos objetos dessa contratação, será(ão) considerada(s) apta(s) para atesto definitivo somente após a conferência de todos os itens e após a conclusão dos respectivos serviços de instalação, desde que não existam outras pendências que impeçam a liberação da(s) mesma(s) para encaminhamento à rotina de pagamento.

28. DAS CONDIÇÕES DE PAGAMENTO

28.1. O pagamento será efetuado após a entrega dos produtos/serviços, por meio de ordem bancária e depósito em conta corrente indicada pela CONTRATADA, à vista do documento fiscal por ela apresentado, devidamente atestado pelo gestor do Contrato, em até 05 (cinco) dias úteis, contados a partir da apresentação do documento fiscal, a contar da emissão de termo detalhado pelo gestor do Contrato;

28.2. Para fins do disposto no item anterior, considerar-se-á como sendo a data do pagamento a data da emissão da ordem bancária;

28.3. No ato do pagamento será efetuada retenção na fonte dos tributos e contribuições elencadas nas disposições determinadas pelos órgãos fiscais e fazendários, em conformidade com a legislação e as instruções normativas vigentes;

28.4. O documento fiscal deverá acompanhar os produtos quando estes forem entregues nos endereços de e-mail constantes do item **19.1**;

28.5. A Contratada que se enquadrar nas hipóteses de isenção ou não retenção de tributos e contribuições deverá comprovar tal situação no ato de entrega do documento fiscal;

28.6. A Contratada optante pelo SIMPLES, para fins do disposto no item anterior, deverá comprovar tal condição mediante a apresentação, em duas vias, da Declaração a que se refere o artigo 6º da Instrução Normativa nº 1.234 de 11/01/2012, da Secretaria da Receita Federal, com as alterações implementadas pelas Instruções Normativas nº 1540 de 05/01/2015 e nº 1.552 de 02/03/2015;

28.7. A Contratada deverá manter, durante toda a vigência do Contrato, as condições de habilitação e qualificação exigidas na presente Licitação, sob pena de rescisão contratual, execução da garantia, além da aplicação das penalidades contratualmente previstas;

28.8. A manutenção das condições de habilitação e qualificação acima referidas será verificada quando da realização de cada pagamento;

28.9. O documento fiscal que for apresentado com erro será devolvido à Contratada para retificação e reapresentação, acrescentando-se, no prazo fixado no item **29.1**, os dias que se passarem entre a data da devolução e a da reapresentação;

28.10. No caso de prestação dos serviços descritos nos itens previstos no inciso XX do art. 14 da Lei Municipal nº 691/1984, alterada pela Lei nº 3.691/2003, na redação da Lei nº 7.000/2021, a Contratada não localizada no Município do Rio de Janeiro estará sujeita à retenção do Imposto sobre Serviços de Qualquer Natureza, no ato do pagamento;

28.10.1. Para fins de identificação da situação prevista no item **29.9**, a Contratada deverá informar, em campo próprio do documento fiscal de cobrança, o código e a descrição do serviço prestado.

29. DA FISCALIZAÇÃO E ACOMPANHAMENTO DA EXECUÇÃO CONTRATUAL

29.1. O Contratante nomeará os responsáveis pela fiscalização e acompanhamento do Contrato, na forma do que estabelece o artigo 29 da Instrução Normativa n° 01/2019/SGD/ME, os quais exercerão como representantes da Administração, toda e qualquer ação de orientação geral, acompanhamento e fiscalização deste Contrato;

29.2. Compete à Fiscalização, entre outras atribuições:

29.2.1. Verificar a conformidade da execução contratual com as normas específicas e se os procedimentos e materiais empregados são adequados para garantir a qualidade desejada dos serviços;

29.2.2. Ordenar à Contratada que corrija, refaça ou reconstrua as partes dos serviços executados com erros, imperfeições ou em desacordo com as especificações;

29.2.3. Acompanhar e aprovar os serviços executados.

29.3. A ação da fiscalização não exonera a Contratada de suas responsabilidades contratuais e legais;

29.4. A Contratada se submeterá à mais ampla e irrestrita fiscalização por parte do Contratante, quanto à execução dos serviços prestando todos os esclarecimentos solicitados;

29.5. As irregularidades detectadas pela fiscalização serão comunicadas por escrito à Contratada, para sua pronta correção ou adequação.

30. DA TRANSFERÊNCIA DE CONHECIMENTO

30.1. Não se aplica, por se tratar de contratação emergencial de um produto que já encontra-se instalado.

31. DOS DIREITOS DE PROPRIEDADE INTELECTUAL E AUTORAIS DOS PRODUTOS GERADOS POR OCASIÃO DA EXECUÇÃO DO CONTRATO

31.1. Não se aplica, considerando que não se trata de desenvolvimento de novos softwares (produtos).

32. DA QUALIFICAÇÃO OU FORMAÇÃO TÉCNICA DOS PROFISSIONAIS ENVOLVIDOS NA EXECUÇÃO DO CONTRATO

32.1. Não se aplica pelas questões informadas no 30.1.

34. DAS PENALIDADES E SANÇÕES ADMINISTRATIVAS

34.1. Conforme o Edital.

35. DO PRAZO DE VIGÊNCIA DA GARANTIA DE BENS E/OU SERVIÇOS

35.1. O prazo da garantia será de 3 (três) meses contados da data do Termo de Recebimento Definitivo das licenças.

36. DO PRAZO DE VIGÊNCIA CONTRATUAL

36.1. A contratação terá validade de 3 (três) meses.

37. DAS ESTIMATIVAS DE PREÇOS DA CONTRATAÇÃO

37.1. Conforme pesquisa de preços a ser realizada.

38. DA ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

38.1 As despesas decorrentes da aquisição das licenças correrão à conta dos recursos específicos consignados no Orçamento Geral da União, conforme especificado abaixo:

Item	Fonte Pagadora	PTR	Classificação da Despesa
2.2.1	TRF2 e SJRJ	SEGO	33.90.40.06 – locação de softwares
2.2.2	TRF2 e SJRJ	SEGO	33.90.40.06 – locação de softwares

39. DA CONFIDENCIALIDADE E SIGILO DAS INFORMAÇÕES

39.1. A Contratada deverá observar rigorosamente todas as normas e procedimentos de segurança adotados no ambiente do Contratante;

39.2. São vedadas a divulgação, a reprodução ou a utilização de quaisquer informações, a qualquer título, exceto quando previamente autorizadas;

39.3. São vedadas a cópia, reprodução, divulgação ou a utilização de quaisquer conteúdos de manuais, documentações ou processos administrativos e judiciais, a qualquer título, exceto quando previamente autorizadas;

39.4. A Contratada deverá assinar termo de responsabilidade e sigilo, conforme previsto no Edital.

40. APROVAÇÃO E ASSINATURA

Papel	Nome	Matr.	Setor
Integrante Requisitante (titular):	Marcus Vinícius do P. Azevedo	11728	DIREM
Integrante Requisitante (suplente):	Pergentino Joaquim Alves Neto	12049	SITI
Integrante Técnico (titular):	Luis Carlos de Freitas	12025	AGSI
Integrante Técnico (suplente):	Ana Luisa Carneiro da SIlva	11066	AGSI
Integrante Administrativo (titular):	Gabriel de Farias Antunes	11833	DIMAT
Integrante Administrativo (suplente):	Leonardo Pastro Vieira	11795	DIMAT

CONTRATAÇÃO Nº 000/ 2025

PROCESSO SEI 0010031-69.2025.4.02.8000

A empresa contratada deverá encaminhar junto com a proposta comercial e a documentação técnica do produto, a planilha de comprovação ponto a ponto dos principais itens, conforme descrito abaixo:

Item	Informar página do manual e texto comprobatório	Observação

17.1.2.1 O serviço de atualização das licenças será prestado dentro do período de suporte e consiste na disponibilização via Internet para o CONTRATANTE de todas as versões (*upgrades*), atualizações (*releases*) e correções (*updates*), de forma a manter a solução permanentemente atualizada, bem como, no fornecimento de manuais e boletins técnicos com informações que assegurem a plena utilização dos produtos licenciados sem custo adicional para o CONTRATANTE.		
17.1.2.2 Os serviços de proteção e de atualização das assinaturas e mecanismos de segurança deverão funcionar em regime 24x7x365.		
17.1.3.1 A SOLUÇÃO ofertada deverá ser de uma única empresa desenvolvedora de software de modo que tanto o suporte à SOLUÇÃO quanto as funcionalidades sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento.		
17.1.3.2 – Os servidores de gerenciamento da SOLUÇÃO deverão possibilitar a distribuição de carga e administração em níveis hierárquicos (primário e secundário), em grupos lógicos independentes da estrutura de domínio da rede, de acordo com regiões geográficas, departamentos, etc.		
17.1.3.3. Deverá suportar comunicação cliente/servidor através dos protocolos de rede TCP/IP		
17.1.3.4. Deverá fornecer proteção e remoção integrada, através de uma única SOLUÇÃO, contra vírus, trojans, worms de rede, spywares, adwares e rootkits, bem como incorporar funcionalidades de firewall pessoal e IPS (intrusion Prevention System).		
17.1.3.5. Deverá fornecer proteção de ameaças da Web através de serviço de reputação de site.		
17.1.3.7. Possibilidade de efetuar backup da base de dados da solução.		
17.1.3.8. Possuir solução de File Reputation (reputação de arquivos), integrada e gerenciada através da console do antivírus, cancelando o download ou execução do arquivo, de forma automática caso o mesmo tenha conteúdo malicioso, baseado na resposta à consulta da base da empresa desenvolvedora da SOLUÇÃO.		
17.1.3.9. Possibilidade de configuração de bloqueio de acesso aos sites maliciosos pela console de gerenciamento.		
17.1.3.10. Possibilidade de criar blacklists e whitelists de URLs para estações pela console de gerenciamento.		
17.1.3.11. Deverá realizar scanner de ameaças do tipo completa (full).		

17.1.3.12. Deverá ser fornecida no idioma Inglês-US e português do Brasil.		
17.1.3.13. Na medida em que novas versões (*upgrades*), ou correções pontuais (*updates*) de problemas (*bugs*) forem introduzidas pela empresa desenvolvedora de software, a CONTRATADA deverá disponibilizar cópias dessas atualizações (*upgrades* ou *updates*) para que elas sejam incorporadas no ambiente do CONTRATANTE.		
17.1.3.14. A CONTRATADA deverá fornecer informações sobre como o CONTRATANTE terá acesso ao serviço de suporte técnico para abertura de chamado e sobre como obter atualizações da SOLUÇÃO.		
17.1.4.1. Deverá prover mecanismos de instalação em clientes e servidores *Windows* através de *login script* com instalação remota a partir da console ou através da rede.		
17.1.4.2. Deverá prover mecanismos de customização dos pacotes de instalação em clientes e servidores.		
17.1.4.4. O pacote deverá detectar automaticamente a versão do sistema operacional do computador destino e instalar a SOLUÇÃO correspondente sem a necessidade de intervenção do administrador ou do usuário.		
17.1.4.5. A customização do pacote de instalação deverá permitir que a distribuição seja feita para os computadores em conformidade com a política de configuração determinada pelo administrador, juntamente com as últimas vacinas, em um único processo transparente e silencioso.		
17.1.4.6. Deverá suportar instalações em clientes remotos e móveis (*notebooks*) sem depender de outro *software* ou agente previamente instalado.		
17.1.4.7. Deverá possuir capacidade de detecção de violações na integridade da instalação ou dos arquivos do antivírus instalado nos clientes e servidores.		
17.1.4.8. Deverá possuir uma ferramenta que permita analisar toda a rede e identificar os computadores que porventura não estejam com o antivírus instalado ou atualizado, de acordo com as políticas determinadas na console de administração.		
17.1.4.9. A solução deverá ser capaz de identificar solução de terceiros que esteja instalada no host e realizar a remoção desta no momento da instalação da solução CONTRATADA.		
17.1.4.10. Deverá apresentar administração centralizada de todos os clientes e servidores *Windows* em console única de gerenciamento baseado na tecnologia MMC (*Microsoft Management Console)* ou através de interface WEB.		

17.1.4.11. O console único de gerenciamento deve exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, versão do antivírus, versão dos mecanismos de verificação (*engine*), data da vacina, data da última verificação e endereço IP.		
17.1.4.12. O console único de gerenciamento deverá permitir travamento das configurações em clientes e servidores para que somente o administrador possa alterar a configuração, desinstalar ou parar a SOLUÇÃO.		
17.1.4.13. O console único de gerenciamento deve permitir a proteção de acesso aos servidores de administração do sistema e grupos lógicos de computadores, através de senhas configuradas pelo administrador.		
17.1.4.14. O console único de gerenciamento deve exibir logs e alertas de todos os clientes e servidores, em tempo real, sem a necessidade de exportar ou transferir arquivos manualmente ou através de *batches* entre clientes, servidores e central de gerenciamento.		
17.1.4.15. Possuir capacidade de aplicar mudanças na configuração do antivírus em clientes e servidores *Windows*, com possibilidade de mudança para todos os computadores, para um determinado grupo de computadores ou para um único computador.		
17.1.4.16. As configurações da SOLUÇÃO em clientes e servidores, depois de modificadas na central de administração, deverão ser distribuídas para os computadores, automaticamente, sem a necessidade de uso de agentes externos, *login scripts*, tarefas manuais ou outros módulos adicionais.		
17.1.4.17. As novas configurações deverão ser efetivamente instaladas e ativadas no computador destino sem a necessidade de reinicialização ou *logoff / logon* do usuário.		
17.1.4.18. Deverá possuir capacidade de envio de alertas, no caso de mudanças de configuração, ativação ou desativação do antivírus, atualização de vacinas e incidência de vírus.		
17.1.4.19. O console de gerenciamento deverá ter a capacidade de abrir uma única janela de alerta de vírus com todas as ocorrências, com o intuito de se evitar a exibição de uma nova janela para cada alerta gerado.		
17.1.4.20. A instalação deverá ser possível sem necessidade de reiniciar a estação de trabalho.		
17.1.4.21. Deverá ser possível gerar imagens (modelos padronizados para instalação) de estações de trabalho com a SOLUÇÃO.		

17.1.4.22. Deverá possibilitar o agrupamento de máquinas com configurações específicas.		
17.1.4.23. Deverá realizar a autorreparação de danos causados por *Trojan Horses*, de forma automática, sem necessidade de agentes ou pacotes adicionais. Essa função deverá ser nativa da SOLUÇÃO e automática, dispensando a intervenção do administrador.		
17.1.4.24. Deverá possuir a capacidade de funcionamento e administração independente da ferramenta de gerenciamento centralizado.		
17.1.4.25. Permitir a utilização de fontes de agentes de atualização secundários em localidades remotas com objetivo de minimizar o consumo do *link* durante a atualização de vacinas; Estes agentes devem ser configurados através da própria console de gerenciamento sem a necessidade de intervenção local ou instalação de outro *software.*		
17.1.4.26. Deverá permitir a varredura dos dispositivos removíveis e periféricos (pen drives, *USB, memórias flash, etc.*), mesmo com a política de bloqueio total ativa.		
17.1.4.27. O console único de gerenciamento deverá permitir a criação de usuários com diferentes níveis de administração.		
17.1.4.28. O console único de gerenciamento deverá permitir integração com o *Active Directory* para identificar máquinas presentes no AD e que não tenham a ferramenta de antivírus instalada, possibilitando ainda a instalação automática da ferramenta para garantir a integridade da rede.		
17.1.4.29. Proteção contra desinstalação e desativação não autorizada da SOLUÇÃO.		
17.1.4.30. Permitir a instalação em ambientes em *Cluster Microsoft.*		
17.1.4.31. Configuração de *Dashboard* com medição do nível de atualização do ambiente ou do nível de cumprimento de política de segurança previamente definida.		
17.1.5.1. Capacidade de atualizar remotamente e em tempo real a vacina e *engine* da SOLUÇÃO, em um único pacote para todas as plataformas suportadas, sem a necessidade de utilização de *login scripts*, agendamentos nas estações ou intervenção do usuário e sem requerer reinicialização do computador ou do serviço Antivírus para aplicação das atualizações.		
17.1.5.2. As atualizações deverão ser feitas a partir de comunicações agendadas ou manuais, entre o servidor de administração e o centro de pesquisas da empresa desenvolvedora da SOLUÇÃO, com mecanismos de checagem de autenticidade e com periodicidade mínima semanal.		

17.1.5.3. Deverá prover mecanismos de distribuição de vacinas para toda a rede a partir de servidor de administração, de forma agendada e tempo real, e com pacotes incrementais, de forma a prevenir a alta utilização de banda de rede.		
17.1.5.4. Deverá ter mecanismos de configuração para o agendamento do envio de vacinas, com tolerância a falhas, para que a tarefa de atualização seja executada dentro de um período determinado, após o horário pré-agendado, e com o intuito de garantir a atualização de clientes e servidores que estivessem anteriormente indisponíveis (desligados, em processo de reinicialização, etc.).		
17.1.5.5. A tarefa de atualização das vacinas deverá possuir mecanismos de randomização, baseados em dias da semana, minutos ou dias, após o horário pré- agendado da atualização, diminuindo assim o tráfego de rede gerado pela SOLUÇÃO no processo de atualização.		
17.1.5.6. O processo de atualização deverá prover mecanismos de configuração para que os clientes façam a busca por novas vacinas, nos servidores de antivírus, em intervalos periódicos e em escala de minutos.		
17.1.5.7. Capacidade de executar a volta imediata para a vacina anterior, através da console de gerenciamento, de forma silenciosa e sem intervenção do usuário, para o caso de a vacina atual apresentar problemas.		
17.1.6.1. Compatível com plataformas existentes no ambiente de TIC do CONTRATANTE.		
17.1.6.2. Rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados, incluindo sessões *DOS* abertas pelo *Windows*, bem como servidores *Linux*.		
17.1.6.3. Rastreamento manual com interface *Windows*, customizável, com opção de limpeza.		
17.1.6.4. Capacidade de detecção de vírus desconhecidos da vacina mais atual, inclusive de macros do *MS Office*, utilizando análise heurística, análise comportamental ou aprendizado de máquina (*machine learning*).		
17.1.6.5. Detecção de programas maliciosos como *spyware*, programas de propaganda, ferramentas como *password crackers*, dentre outros.		
17.1.6.6. Detecção e reparo de arquivos contaminados, mesmo compactados por ZIP, CAB e ARJ.		
17.1.6.7. Permitir configurar ações a serem tomadas na ocorrência de vírus, incluindo, dentre outras, reparar, deletar, mover para a área de Isolamento (quarentena) e ignorar.		
17.1.6.8. Possibilidade de quarentenar o arquivo suspeito antes de limpá-lo.		

17.1.6.9. Rastreamento remoto, de modo manual ou agendado.		
17.1.6.10. Possuir mecanismos de área de isolamento de arquivos para vírus desconhecidos ou sem possibilidade de reparação (área de quarentena).		
17.1.6.11. A área de isolamento deverá remover o arquivo infectado do computador de origem da suspeita de infecção.		
17.1.6.12. Deverá existir a possibilidade de envio de amostras para o centro de pesquisas da empresa desenvolvedora da SOLUÇÃO.		
17.1.6.13 A resposta da empresa desenvolvedora da SOLUÇÃO deverá prover vacina para a amostra enviada que deverá ser adicionada às vacinas existentes, além de tentar reparar, os arquivos isolados na área de quarentena.		
17.1.6.14. A área de isolamento deverá possibilitar a devolução dos arquivos livres de vírus que tenham sido colocados em quarentena para seus pontos de origem.		
17.1.6.15. Capacidade para, em caso de epidemia, bloquear acesso a pastas compartilhadas, a portas TCP e UDP, e escrita em diretórios e arquivos específicos, restaurando as configurações originais ao término da epidemia de forma automática através de políticas recebidas da empresa desenvolvedora da SOLUÇÃO ou de forma manual pela console de gerenciamento.		
17.1.6.16. Possibilidade de colocar arquivos e diretórios em listas de exclusões para não serem verificados pelo antivírus.		
17.1.6.17. Possibilidade de bloquear aplicações com base no nome, diretório ou extensão do arquivo ou também com base no *hash* da aplicação.		
17.1.6.18. Possibilidade de proteger o computador permitindo que somente determinadas aplicações (com base no *hash*) possam ser executadas.		
17.1.6.19. Notificação automática ao administrador em caso de epidemia de vírus.		
17.1.6.20. *Firewall* com capacidade de verificação dos pacotes que estão entrando e/ou saindo da estação de trabalho, com detecção e bloqueio de ataques de *malwares* que exploram vulnerabilidades em *software.*		
17.1.6.21. Capacidade de detecção de ameaças que utilizam algoritmos de compactação em tempo real não padronizados com objetivo de não serem identificados.		
17.1.6.22. Permitir o reinício automático dos serviços do antivírus caso esse tenha sido parado devido a algum código malicioso, sem a necessidade da intervenção do administrador.		

17.1.6.23. Permitir autoproteção ao cliente de antivírus em nível de registro, arquivos de programa e processos.		
17.1.6.24. Capacidade de identificar a origem (servidores ou estações) de ataques de *malwares* na rede local.		
17.1.7.1. Permitir o envio de dados de telemetria para a console continuamente		
17.1.7.2. Permitir o envio de dados de telemetria a partir da criação e edição de arquivo independentemente do tipo de extensão.		
17.1.7.3. Apresentar todas as informações relevantes de um incidente na tela de detalhes do alerta, com, pelo menos, as seguintes informações: Usuários, Ativos, Domínios, IPs, Hashes, Processos ou Técnicas/Táticas identificadas.		
17.1.7.4. Identificar se um processo em execução é seguro ou não por, pelo menos, um dos seguintes métodos: Sistema de reputação do fabricante, Análise de comportamento ou Regras de indicadores.		
17.1.7.5. Permitir a geração de alertas a partir de alertas de detecção de comportamento (Behavior Detection) baseado em dados de telemetria obtidos de agente e tráfego de rede do endpoint.		
17.1.7.6. Proteger contra técnicas de exploração de memória.		
17.1.7.7. Bloquear ataques envolvendo reverse shell.		
17.1.7.8. Bloquear ataques envolvendo exploração de vulnerabilidades de Serialização/Desserialização.		
17.1.7.9. Permitir a remoção de arquivos maliciosos em repouso.		
17.1.7.10. Permitir a customização de consultas por meio de API, possibilitando a geração de relatórios personalizados.		
17.1.7.11. Permitir a exportação de relatórios.		
17.1.7.12. Manter cache de eventos, alertas e telemetria no endpoint mesmo após sua reinicialização, até que seja possível enviar à console de gerência.		
17.1.7.13. Detectar ataques de força bruta para autenticação de endpoints.		
17.1.7.14. Detectar o uso indevido de DLL's confiáveis.		

17.1.7.15 A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas: 17.1.7.15.1 Impedir a execução de objetos. 17.1.7.15.2 Isolamento de host. 17.1.7.15.3 Excluir objeto do host ou grupo de hosts. 17.1.7.15.4 Encerrar um processo no dispositivo. 17.1.7.15.5 Colocar um objeto em quarentena. 17.1.7.15.6 Execute a verificação do sistema. 17.1.7.15.7 Execução remota de programa/processo/comando. 17.1.7.15.8 Iniciar a varredura IoC para um grupo de hosts.		
17.2.1.1. Instalação nas plataformas Microsoft Windows 2012R2 Server até a mais atual existente.		
17.2.1.2. Suporte a Microsoft Exchange 2013 e todas as demais versões do Microsoft Exchange até a mais atual existente.		
17.2.1.3. Rastreamento em tempo real, para arquivos anexados a mensagens do Microsoft Exchange, antes de entregar a mensagem na caixa postal do(s) destinatário(s);		
17.2.1.4. Rastreamento manual às pastas do Exchange, com opção de limpeza.		
17.2.1.5. Programação de rastreamentos automáticos do Exchange.		
17.2.1.6. Gerar registro (log) dos eventos de vírus em arquivo com limite de tamanho opcional.		
17.2.1.7. Gerar notificações de eventos de vírus através de mensagens do Exchange para quem enviou e quem recebeu a mensagem, e para um Administrador (usuário opcional).		
17.2.1.8. Identificação de remetente e destinatário das mensagens.		
17.2.1.9. Permitir bloqueios baseados no tipo de arquivo, nome do arquivo e tamanho do arquivo.		
17.2.1.10. Permitir a instalação em ambientes em Cluster Microsoft.		

Documento assinado eletronicamente por **MARCUS VINICIUS DO PATROCINIO AZEVEDO**, **Diretor**, em 22/05/2025, às 14:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIS CARLOS DE FREITAS**, **Assessor**, em 22/05/2025, às 15:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **GABRIEL DE FARIAS ANTUNES**, **Técnico Judiciário**, em 22/05/2025, às 16:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf2.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0999365** e o código CRC **FB39D6BC**.