PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

FRANCISCO JONATHAN REBOUCAS MAIA
DIVANIA MARIA ALCANTARA SOARES
ROBSON TEIXEIRA DA SILVA
JOAO PAULO COLARES DE ANDRADE

Estudos Preliminares

Segurança de endpoints

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

Sumário

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (Art.14)

Contextualização

O TRT7 possui em operação um servidor do software de segurança para endpoints KASPERSKY com 1.850 licenças adquiridas em 2018, que expiraram em 21/06/2021 e tiveram sua validade prorrogada para 28/09/2021. De modo a prover a segurança das informações, os softwares de segurança para os endpoints demandam sua instalação em nos microcomputadores do tipo desktop e notebooks e nos servidores de rede Windows (físicos ou virtuais) e, portanto beneficiando todas as unidades do Tribunal.

Em 2018, existiam cerca de 1767 equipamentos do tipo microcomputador, entre *desktops* (computadores de mesa) e *notebooks* (computadores móveis), em utilização no ambiente de rede do TRT7. Adicione-se a esse quantitativo cerca de 75 computadores servidores em funcionamento nos *datacenters* da Sede, Fóruns e Varas do Trabalho distribuídos pelo estado.

Conforme levantamento realizado pela SETIC, no período próximo ao previsto para expiração das licenças atuais (21/06/2021), o Tribunal possui 1600 desktops, 210 notebooks e cerca de 103 novos notebooks serão adicionados ao parque por meio de processo de aquisição que está em andamento. Nesse novo cenário, teríamos 1913 computadores em utilização pelos usuários até o final do ano de 2021. Ainda conforme o levantamento, não foram identificadas demandas que resultem crescimento extraordinário e que impliquem em grande aumento da quantidade de microcomputadores, apenas a evolução e renovação de parque observada nos últimos anos.

Comparando os quantitativos de 2018 e 2021, pode-se observar um crescimento de aproximadamente 8,25% no total de microcomputadores.

Calculando uma taxa de crescimento anual, com base no valor de 8,25% por 3 (três) anos, e projetando para o período previsto de vigência da contratação alvo deste estudo, teremos um crescimento de cerca de 11% para os próximos 4 (quatro) anos. Assim, será necessário adquirir 2.124 licenças para uso nos microcomputadores do TRT 7a Região.

Em relação ao quantitativo de computadores servidores que utilizam a solução de segurança, foi observada certa estabilidade do total de equipamentos em execução nos últimos 3 anos, perfazendo a utilização de cerca de 75 dispositivos. Considerando cenário de consolidação de serviços previsto para os próximos anos, em que alguns servidores concentrarão aplicações executadas atualmente em mais de uma máquina, não haverá necessidade de projetar crescimento quantitativo para esse tipo de *endpoint*.

Assim, contemplando 2124 licenças para microcomputadores, 75 para servidores e considerando o registro de 2200 licenças no edital de registro de preços do TRT 13a Regiao, do qual este regional é co-participante, será necessário adquirir 2200 licenças em acordo com as necessidades elencadas acima.

Trata-se de uma demanda de caráter permanente, com renovações periódicas de tecnologia e/ou licenciamento, pois a inexistência de solução de segurança representaria riscos diretos aos 3 três) pilares essenciais para manutenção da segurança da informação, que são a disponibilidade, integridade e confidencialidade da informação. Estações de trabalho ou servidores de rede inoperantes (indisponíveis) em função de infecção por malware (Vírus de computador, *worms*, *trojan horses* e *spywares*) ou o sequestro de informações por partes de grupos especializados (*ransomware)* trariam prejuízos à prestação dos serviços para a população. As informações e sistemas eletrônicos do Tribunal, se não devidamente protegidos, podem ser

violados, alterados, excluídos ou mesmo sequestrados para pagamento de resgate.

Com o advento da LGPD, a preocupação com a segurança no âmbito da Tecnologia da Informação tem sido redobrada. Sendo assim, prover segurança para os endpoints é um dos caminhos para prevenir a invasão do ambiente computacional e o vazamento de dados.

A necessidade de contratação encontra respaldo no Ato Conjunto CSJT.GP.SG.SETIC.CGGOV nº 71/2018, que estabelece o item **Solução de Antivírus** (Suporte) como um dos itens orçamentários obrigatórios.

Considerando os motivos acima expostos, este presente estudo tratará do planejamento da contratação para atender a demanda por solução de segurança para endpoints (antivírus) buscando alcançar os seguintes objetivos:

- Atender às deliberações e aos atos oriundos do CSJT determinando a execução orçamentária dos itens orçamentários obrigatórios, entre os quais se incluem o antivírus;
- Disponibilizar um ambiente computacional seguro minimizando os riscos quanto às ameaças eletrônicas, tais como vírus, worms, trojans, spywares, ransomwares;
- Garantir a integridade e disponibilidade dos sistemas, principalmente PJe;
- Reduzir os riscos de que agentes maliciosos como vírus e outros propiciem a invasão do ambiente computacional do TRT7, provocando o comprometimento de informações ou roubo de dados;

- Reduzir os riscos que um incidente de segurança de TIC aconteça, prejudicando a reputação institucional do TRT7.

1.1 Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

De forma resumida, a demanda compõe-se de solução de segurança de endpoints, sua instalação no ambiente do TRT7 e consequente desinstalação da solução anterior, além de treinamento para equipe técnica.

1.1.1 Requisitos de negócio

- Alta disponibilidade dos recursos e sistemas de TIC, segurança do ambiente de TIC protegido contra ameaças eletrônicas, tais como vírus, worms, trojans, spywares, ransomwares.

1.1.2 Requisitos funcionais

- Proteção antimalware de arquivos;
- Firewall de host;
- Controle de execução de aplicativos;
- Controle de dispositivos instalados nos hosts através de interfaces USB, Bluetooth, rede, etc;
- Integração com Vmware e Hyper-V para proteção de máquinas virtuais;
- Controle de navegação web;
- Uso de informações atualizadas de ameaças disponíveis na nuvem;
- Todos os módulos devem ser do mesmo fabricante;
- Gestão de crise (Epidemia);
- Consolidação de informações sobre códigos maliciosos com mapa de infecção dentro do parque;

- Deve prover uma console de gerenciamento visual (interface gráfica) centralizada;
- Clientes para Sistemas Operacionais Windows, Linux (Red Hat, CentOS, Oracle Linux, Ubuntu), Mac OS e Android;

1.1.2.1 Requisitos gerais para o software de segurança para estações de trabalho e servidores e para o software para ambientes virtualizados

1.1.2.1.1. O console de gerenciamento deve estar disponível para instalação On-Premise (infraestrutura da licitante) ou utilização em nuvem (infraestrutura do fabricante).

1.1.2.1.1.1. Para o caso de appliance virtual, deverá suportar no mínimo o Hypervisor VMWare vSphere 6.7 ou superior;

1.1.2.1.1.2. Para o caso de instalação em sistema operacional Windows, deverá ser compatível, no mínimo, com a versão Microsoft Windows Server 2016 ou superior.

1.1.2.1.2. A solução deve possuir console de gerenciamento visual (interface gráfica) centralizada;

1.1.2.1.3. O Console de gerenciamento deve conter:

1.1.2.1.3.1. Painel para monitoramento;

1.1.2.1.3.2. Capacidade de criação de relatórios;

1.1.2.1.3.3. Mecanismo para envio de notificações administrativas (e-mail);

1.1.2.1.4. Deve permitir inventário das máquinas gerenciadas pela solução;

1.1.2.1.5. O console de gerenciamento deve mostrar quantos dispositivos estão sendo gerenciados e quais seus sistemas operacionais;

1.1.2.1.6. Deve possuir a capacidade de autenticação dos usuários do console de gerenciamento através do Microsoft Active Directory.

1.1.2.1.6.1. Deve permitir a definição de perfis com diferentes níveis de privilégios de administração da solução, baseados em usuários ou grupos do Microsoft Active Directory;

1.1.2.1.6.2. Capacidade de exportar relatórios para, no mínimo 2, dos seguintes tipos de arquivos: PDF, HTML e CSV;

1.1.2.1.6.3. Capacidade de enviar e-mails para contas específicas, em caso de algum evento;

1.1.2.1.6.4. O console de gerenciamento deve fornecer as seguintes informações dos computadores protegidos:

1.1.2.1.6.4.1. Horário da última conexão da máquina com o servidor administrativo ou, no mínimo, o tempo decorrido desde a última conexão;

1.1.2.1.6.4.2. Data e horário da última verificação executada na máquina;

1.1.2.1.6.4.3. Se a solução está instalada;

1.1.2.1.6.4.4. Versão do antivírus instalado na máquina;

1.1.2.1.6.4.5. Se o antivírus está atualizado;

1.1.2.1.6.4.6. Nome do computador;

1.1.2.1.6.4.7. Domínio ou grupo de trabalho do computador;

1.1.2.1.6.4.8. Sistema operacional e Service Pack/Build;

1.1.2.1.6.4.9. Endereço IP.

1.1.2.1.7. Capacidade de instalar remotamente a solução nas estações (endpoints) e servidores Windows, através de compartilhamento administrativo, login script ou GPO do Microsoft Active Directory, no mínimo;

1.1.2.1.8. Capacidade de gerar pacotes auto-executáveis para a instalação do software para gerenciamento, além de automatização para instalação de todos os módulos e informações necessárias para o funcionamento do produto (licenças, configurações, etc);

1.1.2.1.9. Capacidade de importar a estrutura do Microsoft Active Directory para a descoberta de máquinas da rede corporativa;

1.1.2.1.10. Capacidade de monitorar a rede, em diferentes sub redes, a fim de encontrar máquinas novas, para a instalação automática da solução de segurança;

1.1.2.1.11. Deve ser capaz de eleger qualquer computador cliente ou servidor como repositório de vacinas e de pacotes de instalação, sem a necessidade de instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar o tráfego da rede;

1.1.2.1.12. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar o tráfego de link entre sites diferentes;

1.1.2.1.13. Deve permitir a herança de tarefas e políticas na estrutura de hierarquia de servidores administrativos;

1.1.2.1.14. Capacidade de realizar atualização incremental de vacinas nos computadores clientes a partir da rede local e da Internet;

1.1.2.1.15. A atualização incremental de vacinas deve ser disponibilizada, no mínimo, com frequência diária;

1.1.2.1.16. A solução deve possuir integração com o Active Directory, de maneira a permitir a definição de políticas diferentes, baseadas em usuários ou grupos;

1.1.2.1.17. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

1.1.2.1.18. Deve armazenar histórico das alterações feitas em políticas;

1.1.2.1.19. Deve permitir a realocação de máquinas novas na rede para um determinado grupo utilizando os seguintes parâmetros:

1.1.2.1.19.1. Nome do computador;

1.1.2.1.19.2. Range de IP;

1.1.2.1.19.3. Sistema Operacional;

1.1.2.1.20. Caso a solução ofertada não atenda na totalidade os itens aqui referidos, será permitido a composição com outras soluções a fim de atender na plenitude dos itens aqui descritos;

1.1.2.1.21. Deve possuir uma base de inteligência global, do próprio fabricante, sobre campanhas de ameaças existentes;

1.1.2.1.22. Deve ser capaz de dar visibilidade sobre campanhas de ameaças globais;

1.1.2.1.23. A solução deve ser capaz de proporcionar a busca por ameaças baseadas em IOCs;

1.1.2.1.24. Deve ser capaz de indicar quantos e quais dispositivos dentro da empresa estão vulneráveis a determinada ameaça;

1.1.2.1.25. Deve ser capaz de mostrar o nível de postura de segurança da organização, em relação às políticas aplicadas no ambiente protegido.

1.1.2.1.26. Cada ameaça identificada pela solução deverá possuir as seguintes informações:

1.1.2.1.26.1. Detalhes do ataque;

1.1.2.1.26.2. IOCs;

1.1.2.1.26.3. Detalhes do Impacto no ambiente;

1.1.2.1.26.4. Endpoints afetados;

1.1.2.1.26.5. Comportamento da ameaça.

1.1.2.2 Requisitos para o software de segurança para estações de trabalho

1.1.2.2.1 Aspectos gerais

1.1.2.2.1.1. Prover segurança para as estações de trabalho (endpoints), sejam físicas ou em ambiente virtualizado;

1.1.2.2.1.2. Se comunicar com console central de gerenciamento, de forma que seja possível gerenciar todas as funcionalidades;

1.1.2.2.1.3. Detectar e eliminar programas maliciosos (malwares), tais como vírus, ransomware, spywares, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

1.1.2.2.1.4. Identificar e proteger contra eventuais vulnerabilidades dos sistemas operacionais e aplicações;

1.1.2.2.1.5. Deve detectar e eliminar programas maliciosos em:

1.1.2.2.1.5.1. Processos em execução em memória principal (RAM);

1.1.2.2.1.5.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

1.1.2.2.1.5.3. Arquivos compactados, em tempo real ou no ato de sua execução, com os seguintes formatos: ZIP, EXE, ARJ, RAR, e CAB;

1.1.2.2.1.5.4. Detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex.

1.1.2.2.1.6. Capacidade de detecção heurística de malwares desconhecidos;

1.1.2.2.1.7. Possuir tecnologia de Machine Learning de pre-execution, run time machine e post-execution;

1.1.2.2.1.8. Deve prover, no mínimo, as seguintes proteções:

1.1.2.2.1.8.1. Antivírus de arquivos;

1.1.2.2.1.8.2. Antivírus web (verificação de sites e downloads contra malwares);

1.1.2.2.1.8.3. Firewall de host com HIPS (Host Intrusion Prevention System) e/ou HIDS (Host Intrusion Detection System);

1.1.2.2.1.8.4. Proteção contra ataques aos serviços/processos do antivírus;

1.1.2.2.1.8.5. Controle de dispositivos;

1.1.2.2.1.8.6. Controle de execução de aplicativos;

1.1.2.2.1.8.7. Controle de acesso a sites por categorias (Adulto, Jogos, etc);

1.1.2.2.1.8.8. Prevenção contra exploração de vulnerabilidades.

1.1.2.2.1.8.9. Capacidade de integração com a Antimalware Scan Interface (AMSI).

1.1.2.2.1.9. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

1.1.2.2.2. Detalhamento das proteções:

1.1.2.2.2.1. Antivírus de arquivos:

1.1.2.2.2.1.1. Verificar todos os arquivos criados, acessados ou modificados, inclusive em sessões de linha de comando (DOS ou shell) abertas pelo usuário;

1.1.2.2.2.1.2. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

1.1.2.2.2.1.3. Deve possuir Módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

1.1.2.2.2.1.4. Deve possuir Módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro;

1.1.2.2.2.1.5. Capacidade para definir escopo de varredura/rastreamento: todos os discos locais, discos específicos;

1.1.2.2.2.1.6. Capacidade de adicionar pastas/arquivos em uma zona de exclusão, a fim de excluí-los da verificação;

1.1.2.2.2.1.7. Possibilidade de definir frequência de varredura;

1.1.2.2.2.1.8. Capacidade de realizar a verificação "inteligente" de arquivos, ou seja, somente verificará o arquivo se este for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la apenas a partir da extensão do arquivo;

1.1.2.2.2.1.9. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

1.1.2.2.2.2. Antivírus web:

1.1.2.2.2.2.1. O antivírus web deve ter a capacidade de verificação de tráfego HTTP/HTTPS e scripts (JavaScript, Visual Basic Script, etc.);

1.1.2.2.2.2.2. Capacidade de limitar o acesso a sites da Internet por reputação;

1.1.2.2.2.2.3. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus web;

1.1.2.2.2.2.4. Capacidade de verificar tráfego nos browsers: Internet Explorer, Mozilla Firefox e Google Chrome.

1.1.2.2.2.3. Firewall de host com HIPS e/ou HIDS

1.1.2.2.2.3.1. O módulo de firewall deve conter, no mínimo, dois conjuntos de regras:

1.1.2.2.2.3.1.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas ou, definir o comportamento da filtragem de pacotes, podendo definir pelo menos, mas não limitado a: permitir, bloquear ou bloquear com exceções aos pacotes de rede;

1.1.2.2.2.3.1.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo terá acesso à rede.

1.1.2.2.2.3.2. Deve possuir módulo HIPS e/ou HIDS para proteção/detecção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

1.1.2.2.2.4. Proteção contra Ameaças Avançadas

1.1.2.2.2.4.1. A solução deve permitir a análise comportamental avançada de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware);

1.1.2.2.2.4.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas permitindo sua execução e analisando seu comportamento no endpoint;

1.1.2.2.2.4.3. Deve permitir criar exceções para aplicações confiáveis, evitando que sejam bloqueadas por componentes de detecção;

1.1.2.2.2.4.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;

1.1.2.2.2.4.5. Solução deve manter um cache de reputação local com informações de aplicações conhecidas, desconhecidas e maliciosas;

1.1.2.2.2.4.6. Dentre os comportamentos maliciosos, deve ser capaz de "bloquear" ou "detectar e trazer rastreabilidade sobre":

1.1.2.2.2.4.6.1. Acesso local a partir de cookies;

1.1.2.2.2.4.6.2. Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;

1.1.2.2.2.4.6.3. Criação de threads em outro processo;

1.1.2.2.2.4.6.4. Desativação de executáveis críticos do sistema operacional;

1.1.2.2.2.4.6.5. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;

1.1.2.2.2.4.6.6. Gravação e Leitura na memória de outro processo;

1.1.2.2.2.4.6.7. Modificação da política de firewall do Windows;

1.1.2.2.2.4.6.8. Modificação da pasta de tarefas do Windows;

1.1.2.2.2.4.6.9. Modificação de arquivos críticos do Windows e Locais do Registro;

1.1.2.2.2.4.6.10. Modificação de arquivos executáveis portáteis;

1.1.2.2.2.4.6.11. Modificação de bit de atributo oculto;

1.1.2.2.2.4.6.12. Modificação de bit de atributo somente leitura;

1.1.2.2.2.4.6.13. Modificação de entradas de registro de DLL AppInit;

1.1.2.2.2.4.6.14. Modificação de locais do registro de inicialização;

1.1.2.2.2.4.6.15. Modificação de pastas de dados de usuários;

1.1.2.2.2.4.6.16. Modificação do local do Registro de Serviços;

1.1.2.2.2.4.6.17. Suspensão de um processo;

1.1.2.2.2.4.7. Deve ser capaz de bloquear ou apenas informar quando uma ameaça for encontrada;

1.1.2.2.2.4.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem;

1.1.2.2.2.4.9. Deve possuir modo de ativação da análise comportamental avançada para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

1.1.2.2.2.4.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;

1.1.2.2.2.4.11. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção;

1.1.2.2.2.4.12. Utilizar técnicas de machine learning para detecção de ameaças

1.1.2.2.2.5. Controle de dispositivos:

1.1.2.2.2.5.1. Deve possuir módulo de controle de dispositivos, que permita o bloqueio e a ativação de dispositivos;

1.1.2.2.2.5.2. Capacidade de liberar o acesso a um dispositivo específico sem a necessidade de desabilitar a proteção ou da intervenção local na máquina do usuário;

1.1.2.2.2.5.3. Capacidade de adicionar novos dispositivos por Class ID/Hardware ID.

1.1.2.2.2.6. Controle de execução de aplicativos:

1.1.2.2.2.6.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas e aplicar o controle de execução imposto pela política;

1.1.2.2.2.6.2. Deve ser capaz de realizar um inventário das estações de trabalho protegidas informando todos os executáveis presentes;

1.1.2.2.2.6.3. Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação;

1.1.2.2.2.6.4. Ao detectar um executável, a solução deverá consultar a solução de reputação de arquivos e compartilhamento de informações de segurança;

1.1.2.2.2.6.5. Caso não seja possível efetuar comunicação com a solução de reputação de arquivos e compartilhamento de informações de segurança, o módulo deve realizar consulta de reputação para o Centro de Inteligência do fabricante;

1.1.2.2.2.6.6. Deve ser possível criar uma imagem base para a criação de uma política geral;

1.1.2.2.2.6.7. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;

1.1.2.2.2.6.8. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA- 1).

1.1.2.2.2.6.9. A solução deve suportar as seguintes modalidades de proteção:

1.1.2.2.2.6.9.1. Criação de uma lista de aplicações autorizadas que podem ser executadas, onde todas as demais aplicações são impedidas de serem executadas;

1.1.2.2.2.6.9.2. Criação de uma lista de aplicações não autorizadas que não podem ser executadas;

1.1.2.2.2.6.9.3. Monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.

1.1.2.2.2.6.10. Deve ser capaz de proteger em modo standalone - online ou offline;

1.1.2.2.2.6.11. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do órgão;

1.1.2.2.2.6.12. Permitir o bloqueio de aplicações e os processos que a aplicação interage;

1.1.2.2.2.6.13. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;

1.1.2.2.2.6.14. Permitir monitoração de Hooking de aplicações;

1.1.2.2.2.7. Proteção contra ransomwares:

1.1.2.2.2.7.1. Bloquear a criptografia de arquivos em recursos compartilhados a partir de um processo malicioso, inclusive, que esteja sendo executado em outra máquina;

1.1.2.2.2.7.2. Monitoramento de pastas compartilhadas no ambiente Windows, rastreando o estado dos arquivos armazenados e os protegendo;

1.1.2.2.2.7.3. Na detecção de atividade maliciosa de criptografia por ransomware, o antivírus deve interromper o processo de criptografia e restaurar os arquivos ao seu estado original, impedindo a perda de dados corporativos.

1.1.2.2.3. Características do módulo de reputação de arquivos e compartilhamento de informações de segurança:

1.1.2.2.3.1. Deve ser fornecida em formato de appliance virtual ou existir nativamente no gerenciamento do produto, sem a necessidade de appliance;

1.1.2.2.3.2. Se for entregue no formato de appliance virtual, deve ser compatível no mínimo com ambiente virtualizado VMWare ESXi;

1.1.2.2.3.3. A solução deve possuir capacidade de criar uma reputação local ou utilizar uma já existente em nuvem através da catalogação de todos os executáveis existentes no ambiente;

1.1.2.2.3.4. O servidor de reputação deverá habilitar a troca de informação de ameaças entre os endpoints e servidores protegidos;

1.1.2.2.3.5. A troca de informação de ameaças deve se dar por meio de protocolo performático ou através da console de gerenciamento de forma criptografada;

1.1.2.2.3.6. De forma a permitir menor impacto na rede, para tal método de consulta dos clientes à base de dados poderá ser síncrona ou assíncrona;

1.1.2.2.3.7. A solução deverá apresentar a reputação dos arquivos definida para cada um dos ativos conectados, dentre eles:

1.1.2.2.3.7.1. Reputação local;

1.1.2.2.3.7.2. Reputação do centro de inteligência.

1.1.2.2.3.8. Após análise pela solução o administrador deve ter a possibilidade de:

1.1.2.2.3.8.1. Rastrear em quais estações o arquivo foi executado;

1.1.2.2.3.8.2. Identificar o arquivo como confiável;

1.1.2.2.3.8.3. Identificar o arquivo como desconhecido;

1.1.2.2.3.8.4. Identificar o arquivo como malicioso;

1.1.2.2.3.8.5. Analisar o certificado associado ao arquivo;

1.1.2.2.3.8.6. Identificar o certificado associado como confiável ou malicioso.

1.1.2.2.3.9. Deve ser possível bloquear a execução de arquivos suspeitos no ambiente e informar o usuário por meio de mensagem;

1.1.2.2.3.10. Deve ser capaz de identificar manualmente um arquivo e proibir que ele seja executado no ambiente.

1.1.2.2.4. Módulo de proteção para dispositivos móveis

1.1.2.2.4.1. A solução de "proteção para dispositivos móveis", deve proteger a CONTRATANTE contra as ameaças em dispositivos móveis, Android e iOS, incluindo malwares, ameaças de rede e defesa física dos dispositivos. O objetivo principal desta solução é proteger os usuários móveis, impedindo que ameaças nestes dispositivos possam impactar nos serviços e na rede da CONTRATANTE;

1.1.2.2.4.2. Características Gerais:

1.1.2.2.4.2.1. Deverá ser ofertado como um serviço on-premises (local) ou em console baseado em nuvem de forma a garantir suas funcionalidades independente da rede que o dispositivo estiver conectado;

1.1.2.2.4.2.2. A solução deverá possuir console WEB para administração da solução;

1.1.2.2.4.2.3. Possuir dashboard com os principais indicadores da solução, como Distribuição de níveis de risco, dispositivos em não conformidade, total de dispositivos protegidos e incidentes recentes;

1.1.2.2.4.2.4. Apresentar, nos dashboards, uma visão geral dos riscos examinados nos dispositivos móveis, como ameaças de rede e malwares encontrados;

1.1.2.2.4.2.5. Deverá possuir uma apresentação gráfica referente às informações dos dispositivos registrados na solução;

1.1.2.2.4.2.6. O console deverá apresentar os principais incidentes gerados, contendo todos os detalhes sobre o incidente e o dispositivo que o gerou;

1.1.2.2.4.2.7. Deverá ser compatível com os sistemas operacionais iOS e Android;

1.1.2.2.4.2.8. O cliente da solução deverá estar disponível nas lojas oficiais dos fabricantes, sendo Apple Store para iOS e Play Store para Android ou ser instalado de forma remota através da console de gerenciamento.

1.1.2.2.4.2.9. Permitir configuração no cliente instalado nos dispositivos móveis para que nenhuma informação e alerta seja visível para o usuário final, através de modo não interativo;

1.1.2.2.4.2.10. Deverá possuir as seguintes características mínimas de proteção:

1.1.2.2.4.2.10.1. Proteção contra Malwares:

1.1.2.2.4.2.10.1.1. Proteção em tempo real contra malwares conhecidos e desconhecidos;

1.1.2.2.4.2.10.2. Defesa física:

1.1.2.2.4.2.10.2.1. Identificação de upgrades do sistema operacional;

1.1.2.2.4.2.10.2.2. Identificação de dispositivo com root.

1.1.2.2.4.2.11. Deverá possuir integração com solução de SIEM de mercado;

1.1.2.2.4.2.12. A solução deve apresentar notificações de violações para o usuário final e para os administradores da solução, através de e-mail e notificações Push;

1.1.2.2.5. Compatibilidade

1.1.2.2.5.1. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações de trabalho:

1.1.2.2.5.1.1. Microsoft Windows 8 (e suas edições);

1.1.2.2.5.1.2. Microsoft Windows 8.1 (e suas edições);

1.1.2.2.5.1.3. Microsoft Windows 10 (e suas edições);

1.1.2.2.5.1.4. Sistemas legados em Windows 7.

1.1.2.2.5.2. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para servidores:

1.1.2.2.5.2.1. Microsoft Windows Server 2012 (e suas edições);

1.1.2.2.5.2.2. Microsoft Windows Server 2012 R2 (e suas edições);

1.1.2.2.5.2.3. Microsoft Windows Server 2016 (e suas edições);

1.1.2.2.5.2.4. Microsoft Windows Server 2019 (e suas edições).

1.1.2.2.5.3. A solução deve ser compatível para a funcionalidade de antimalware, no mínimo, com a seguinte distribuição/versão de sistema operacional Linux para estações de trabalho e servidores:

1.1.2.2.5.3.1. Red Hat Enterprise 7.x e superior, 32 e 64 bits;

1.1.2.2.5.3.2. SUSE Linux Enterprise Server 12.x e superior, 32 e 64 bits;

1.1.2.2.5.3.3. Ubuntu 16.04 e superior, 32 e 64 bits;

1.1.2.2.5.3.4. CentOS 7.x e superior, 32 e 64bits;

1.1.2.2.5.3.5. Oracle Linux 7.x e superior, 32 e 64bits;

1.1.2.3 Requisitos para o software de segurança para ambientes virtualizados

1.1.2.3.1 Aspectos gerais

1.1.2.3.1.1. Ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes VMware ESXi e Hyper-V;

1.1.2.3.1.2. Deve prover, no mínimo, as seguintes proteções:

1.1.2.3.1.2.1. Antivírus de arquivos que verifique todos os arquivos criados, acessados ou modificados;

1.1.2.3.1.2.2. Proteção contra ataques aos serviços/processos do antivírus.

1.1.2.3.1.3. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na remota;

1.1.2.3.1.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

1.1.2.3.1.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

1.1.2.3.1.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

1.1.2.3.1.4.3. Leitura de configurações;

1.1.2.3.1.4.4. Modificação de configurações.

1.1.2.3.1.5. Em caso de erros, deve ter a capacidade de criar logs e traces automaticamente, sem necessidade de uso de outros softwares;

1.1.2.3.1.6. Capacidade de adicionar pastas/arquivos em uma zona de exclusão, a fim de excluí-los da verificação;

1.1.2.3.1.7. Capacidade de realizar a verificação inteligente de arquivos, ou seja, somente verificará o arquivo se este for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar apenas a partir da extensão do arquivo;

1.1.2.3.1.8. Capacidade de verificar objetos usando heurística;

1.1.2.3.1.9. Antes de qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

1.1.2.3.2. Compatibilidade

1.1.2.3.2.1. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações servidoras:

1.1.2.3.2.1.1. Microsoft Windows Server 2012 (e suas edições);

1.1.2.3.2.1.2. Microsoft Windows Server 2012 R2 (e suas edições);

1.1.2.3.2.1.3. Microsoft Windows Server 2016 (e suas edições);

1.1.2.3.2.1.4. Microsoft Windows Server 2019 (e suas edições).

1.1.2.3.2.2. A solução deve ser compatível, no mínimo, com as seguintes distribuições/versões de sistemas operacionais Linux para servidores:

1.1.2.3.2.2.1. RedHat Enterprise Linux 7.x e superior, 32 e 64 bits;

1.1.2.3.2.2.2. SUSE Linux Enterprise Server 12 SP1 e superior, 32 e 64 bits;

1.1.2.3.2.2.3. Ubuntu 16.04 LTS e superior, 32 e 64 bits;

1.1.2.3.2.2.4. CentOS 7.x e superior, 32 e 64 bits;

1.1.2.3.2.2.5. Oracle Linux 7.x e superior, 32 e 64 bits;

1.1.3 Requisitos para o serviço de implantação e migração da solução

1.1.3.1. A LICITANTE vencedora será inteiramente responsável pela instalação, atualização ou migração da solução antivírus atualmente em uso pela CONTRATANTE, bem como às despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

1.1.3.2. A instalação, atualização ou migração dos softwares em estações de trabalho poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

1.1.3.3. A instalação, atualização ou migração dos softwares em servidores de rede poderá ser realizada remotamente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

1.1.3.4. A CONTRATANTE poderá autorizar a instalação, atualização ou migração durante o horário de expediente se, ao seu exclusivo critério, entender que não

oferece risco ao funcionamento de sua rede de computadores e serviços em produção;

1.1.3.5. O processo de instalação, atualização ou migração da solução deverá ser acompanhado por servidores da CONTRATANTE;

1.1.3.6. Para garantir que a instalação, atualização ou migração não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante;

1.1.3.7. Em caso de migração de solução, a CONTRATADA deverá:

1.1.3.7.1. Realizar a migração de todas políticas, regras e customizações configuradas no CONTRATANTE;

1.1.3.7.2. A CONTRATADA deverá se reunir com a equipe técnica da CONTRATANTE e elaborar um plano de migração, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço de migração;

1.1.3.7.3. A Migração da solução deverá seguir todos os procedimentos internos da CONTRATANTE, incluindo os processos de registro de mudanças, liberações e incidentes.

1.1.4 Requisitos para o treinamento e atualização tecnológica

1.1.4.1. A CONTRATADA deverá fornecer treinamento com carga horária mínima de 20 (vinte) horas, contemplando a perfeita instalação, operação, manuseio, gerenciamento, configuração e utilização das soluções contratadas;

1.1.4.2. Os treinamentos deverão ser realizados em dias úteis, em horário comercial;

1.1.4.3. O treinamento deverá ser realizado de forma remota. Deverão capacitados, no mínimo, 3 (três) servidores do TRT7;

1.1.4.3.1 A depender da disponibilidade de recursos orçamentários à época da contratação, serão capacitados mais servidores até um total de 10 (dez), incluindo-se o mínimo exigido 1.1.4.3, visando dar maior abrangência ao conhecimento necessário para operação da ferramenta, principalmente para as equipes de suporte técnico.

1.1.4.4. Deverá ser disponibilizado material didático impresso e/ou em mídia digital, sem custo adicional para a CONTRATANTE. Todo material deverá estar, preferencialmente, em língua Portuguesa (Brasil), sendo aceitável o idioma inglês;

1.1.4.5. Deverá ser emitido certificado de participação ao final do curso a cada participante;

1.1.4.6. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato;

1.1.4.7. Caso o treinamento/atualização fornecido não seja considerado satisfatório mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizá-los novamente, sem ônus adicional à CONTRATANTE;

1.1.4.8. A critério da CONTRATANTE, o treinamento poderá ser dividido em turmas;

1.1.4.9. O conteúdo programático deverá englobar, pelo menos, os seguintes assuntos:

1.1.4.9.1. Instalação do ambiente;

1.1.4.9.2. Manutenção básica, intermediária e avançada;

1.1.4.9.3. Configurações básicas e avançadas;

1.1.4.9.4. Verificação de alertas e erros;

1.1.4.9.5. Monitoramento e relatórios.

1.1.5 Requisitos para os Serviços de Suporte Técnico

1.1.5.1. O atendimento aos chamados deverá estar disponível de segunda-feira a sexta-feira, no horário das 8h às 17h, horário de Brasília. A abertura de chamados pelo CONTRATANTE será efetuada por correio eletrônico, por sistema de controle de chamados ou por telefone. A abertura de chamados poderá ocorrer em qualquer horário por email ou sistema de controle de chamados, enquanto por telefone apenas no horário mencionado. No caso de abertura de chamado fora do horário estipulado, a contagem do prazo, para efeitos de nível de serviço (SLA), se dará no próximo dia útil;

1.1.5.2. A assistência técnica em garantia deve garantir o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configuração atualizados, FAQ’s, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca);

1.1.5.3. O suporte técnico do fabricante deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes às plataformas de software e hardware (inclusive virtual) dos produtos;

1.1.5.4. Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, instalação de novas versões, patches e hotfixes, análise de dúvidas sobre melhores práticas de configuração, entre outros;

1.1.5.5. Os prazos de resposta para problemas ocorridos durante o período de suporte estão apresentados na tabela abaixo e são contados do recebimento da notificação de abertura do chamado:

Grau de impacto	Descrição	Tempo máximo para resposta inicial	Tempo máximo para solução
Nível 1 - Alto	Indisponibilidade de uso da solução	2 horas comerciais	1 dia útil
Nível 2 - Médio	Falha, simultânea ou não, de uma ou mais funcionalidades que não cause indisponibilidade, mas apresente problemas de funcionamento e/ou performance da solução	4 horas comerciais	2 dias úteis
Nível 3 - Baixo	Instalação, configuração, atualização de versões e implementações de novas funcionalidades	6 horas comerciais	3 dias úteis

1.1.5.6. Automaticamente e sem custos adicionais, deverá ser possível o acesso ao conteúdo mais recente dos produtos, funcionalidades adicionais e correções de produtos disponibilizadas pelo fabricante;

1.1.5.7. A CONTRATADA deverá manter, durante toda a vigência do prazo de garantia, um “gerente técnico de contas”. O “gerente técnico de contas” deverá ser o ponto de contato entre o FABRICANTE, CONTRATADA e CONTRATANTE para solucionar pendências e questões que não foram resolvidas pelo suporte técnico.

1.1.6. Requisitos de qualificação técnica

1.1.6.1. Para desempenho das atividades relacionadas neste estudo é necessário que a contratada disponha de pelo menos 1 (um) profissional com certificação ou documento/atestado técnico emitido pelo fabricante da solução contratada. Esta solicitação visa garantir que a CONTRATADA tenha plenas condições de elaborar/acompanhar o processo de instalação/configuração do objeto da licitação, assim como manter o nível de suporte técnico necessário durante toda a vigência do contrato;

1.1.6.2. A empresa deverá apresentar documento que comprove ser REVENDA AUTORIZADA do fabricante do software.

1.1.6.2.1. Tal exigência visa proteger o alto investimento feito pela administração na aquisição da solução. Considerando que o escopo do projeto inclui não somente o fornecimento de licenças, mas também o suporte técnico durante 48 meses e que se trata de software fundamental para manutenção da segurança dos dados da instituição, exige-se a declaração de revenda autorizada, visto que tais fornecedores são obrigados a cumprir uma série de requisitos de qualidade determinados pelos fabricantes.

1.1.6.3. Atestado de capacidade Técnico – Operacional: comprovação por parte da empresa licitante de ter realizado fornecimento com características similares ou superiores à do objeto licitado. Esta comprovação se dará obrigatoriamente através dos documentos abaixo descritos:

1.1.6.3.1. Declaração(ões), certidão(ões) ou atestado(s) emitido por pessoas jurídicas de Direito Público ou Privado, referente(s) a fornecimento realizado em qualquer época ou local pela empresa CONTRATADA, comprovando ter

fornecido licenças da solução com prestação de suporte, na quantidade de, pelo menos, 50% (cinquenta por cento) do quantitativo de licenças a ser fornecido.

1.1.6.3.2. Será admitida a apresentação de mais de um atestado que, em somatória, comprove a experiência requerida da empresa no objeto em referência, contemplando todas as características qualitativas exigidas.

1.1.7 Requisitos temporais

1.1.7.1. Deverão ser cumpridos os eventos descritos nas tabelas a seguir, respeitando os prazos máximos estabelecidos, os quais poderão ser antecipados sempre que as circunstâncias assim o permitam:

MARCO	PRAZO (dias úteis)	EVENTO	RESPONSÁVEL	CRITÉRIO DE ACEITE
D0	-----	Assinatura do contrato	TRT7 e CONTRATADA	Contrato assinado
D1	D0 + 10	Reunião de Planejamento	TRT7 e CONTRATADA	Ata de reunião assinada
D2	D0 + 20	Instalação e configuração da solução	CONTRATADA	Solução implantada e funcionando plenamente
D3	D2 + 05	Recebimento Provisório	TRT7	Parecer do Fiscal Técnico
D4	D3 + 05	Recebimento Definitivo	TRT7	Verificação do funcionamento e das especificações dos produtos e serviços entregues

1.1.7.2. O prazo máximo para a entrega e instalação do software será de 30 (trinta) dias úteis, contados a partir da data de assinatura do contrato;

1.1.7.3. Prazo de vigência de 48 (quarenta e oito) meses. Tal prazo reduz o risco de problemas causados por processos de prorrogação contratual que poderiam ocasionar a interrupção do serviço sendo plenamente justificável em razão da criticidade que é a manutenção da segurança dos endpoints. A cada nova contratação em que ocorre mudança de fabricante/software existe também a necessidade de capacitar os técnicos na nova solução, desinstalar o software antigo, configurar e instalar o novo software com grande possibilidade de interrupção na proteção dos referidos dispositivos;

1.1.7.4. Início da prestação dos serviços de suporte e atualização a contar do recebimento definitivo.

1.2 Soluções Disponíveis no Mercado (Art. 14, I, a)

1.2.1 Solução de segurança de endpoints

1.2.1.2. Para atender a demanda de segurança de endpoints (servidores e estações de trabalho), a única possibilidade existente é através de programas desenvolvidos para esta finalidade. Por enquanto não há outra alternativa para prover segurança dos endpoints. De forma resumida, o programa deve ser capaz não só de detectar, mas atuar no impedimento e na remoção de programas considerados maliciosos, como também trabalhar na manutenção da integridade dos endpoints para assim, mantê-los com o maior nível de segurança possível. Tal segurança não deve se resumir apenas à proteção anti-malware. Geralmente inclui recursos como gerenciamento de permissões de instalação, execução e acessos de aplicativos, controle do acesso à rede local e à Internet, controle de dispositivos, detecção e resposta de ameaças.

1.2.1.3. No mercado, há vários produtos para essa finalidade e com características muito semelhantes. A seguir, apresentamos a pesquisa de mercado realizada para esses produtos.

Produto	Fabricante	Valor total para 1850 endpoints -- 48 meses	Valor unitário por endpoint -- 48 meses	Serviço de instalação(*)	Treinamento para 3 pessoas	Valor total da proposta
GravityZone Advanced Security Business	Bitdefender	R$ 148.000,00	R$ 80,00	R$ 92.500,00	R$ 4.500,00	R$ 245.000,00
Kaspersky Endpoint Security for Business SELECT (*)	Kaspersky	R$ 345.950,00	R$ 187,00	--------(**)	----------(**)	R$ 345.950,00
Intercept X Endpoint	SOPHOS	R$ 888.340,00	R$ 480,00 (***)	R$ 8.776,84	R$ 3.267,97	R$ 900.384,81
MVISION Protect Plus MV2	Mcafee	R$ 425.50,00	R$ 230,00	R$ 15.000,00	R$ 15.000,00	R$ 455.500,00

(*) O serviço de instalação deve contemplar a desinstalação da solução anterior e posterior instalação e configuração da nova solução

(**) Alguns itens não foram cotados pois essa solução está atualmente em uso e dispensa os serviços.

(***) valor médio da licença. Este fornecedor em especial diferencia licença de estação de trabalho e licença de servidor de rede para fins de preços.

1.3 Contratações Públicas Similares (Art. 14, I, b)

TRF2 - JF-ES - item: KASPERSKY ENDPOINT SECURITY FOR BUSINESS - SELECT BRAZILIAN EDITION. 1000-1499 NODE 3 YEAR BASE LICENSE / KASPERSKY SECURITY FOR MAIL SERVER BRAZILIAN EDITION. 1000-1499

MAILADDRESS 3 YEAR ADD-ON LICENSE: Quantidade: 1.100. valor unitário R$ 112,00.

UFRGS - Contrato nº 13/2021 - item: Renovação das licenças da solução de segurança para dispositivos fins Kaspersky EndPoint Security for Business Advanced, já implementada e em produção na UFRGS, com 7500 licenças, por um período de 04 (quatro) anos. valor unitário R$ 134,34;

TC-ES - ARP 04/2020 - item: Licença de subscrição da solução de segurança Symantec Endpoint Protection por 36 meses. - Quantidade: 700. valor unitário R$ 213,87.

MP-MG - contrato 200/2020 - item: SUBSCRIÇÃO DE LICENÇA, ATUALIZAÇÃO E SUPORTE DE SOFTWARE DE SOLUÇÃO PARA SEGURANÇA DE ENDPOINTS E SERVIDORES - 36 meses - Quantidade: 9.000. valor unitário R$ 114,44.

SENADO FEDERAL - Contrato 69/2019 - vigência até 27/09/2022 (conforme 2º termo aditivo) - item Prestação de serviço de atualização de versão e suporte técnico, por meio de licenciamento, para 150 (cento e cinquenta) licenças da solução de segurança McAfee Management for Optimized Virtual Environments (MOVE) - Valor unitário da licença por 12 meses - (R$ 22.824,00 /150 unidades = R$ 152,16) - valor estabelecido no 1º termo aditivo.

CRM-SC - PE 06/2021 - item: Aquisição de solução de antivírus corporativo por 12 (doze) meses, renováveis até o prazo legal de 48 meses, incluindo garantia de atualização contínua, serviços de treinamento, instalação, configuração, manutenção corretiva e preventiva e suporte técnico especializado para proteção dos equipamentos do ambiente de TIC do CRM-SC. Valor unitário da licença por 12 meses - R$ 88,00 - quantidade: 150 (cento e cinquenta). No item 2.1.5.2 do termo de referência está disposto que esse item é para máquinas virtuais.

Ministério Público do Estado do Mato Grosso - Contrato 93/2020 - item: Serviço de suporte e atualização de versão do Kaspersky Endpoint Security for

Business - Advanced, a ser prestado pelo fabricante pelo período de 36 (trinta e seis) meses. Valor unitário da licença - R$ 103,00. A versão Advanced do Kaspersky inclui máquinas virtuais. Corrobora esse entendimento o disposto no item 2.2 do edital do Pregão 78/2020, afirmando que a solução da Kaspersky contratada provê segurança para servidores virtuais.

TRT13 - PE 11/2021 - item: Licença de software de segurança para endpoints (estações de trabalho, dispositivos móveis e servidores físicos) + Console de Gerenciamento / Garantia /Atualizações / Suporte Técnico /Manutenção Preventiva e Corretiva por 48 (quarenta e oito) meses - Quantidade: 82.809. valor unitário R$ 125,60.

Não foram encontradas outras ARPs válidas com o mesmo objeto.

1.3.1. Análise dos preços encontrados

Em primeiro lugar, é importante destacar o fato da licitação do TRT13 resultar em uma ARP da qual o TRT7 é coparticipante. Nela, há um alinhamento perfeito entre os requisitos e as necessidades de contratação de ambos os Tribunais. Além disso, trata-se de uma licitação recente, com preços válidos até **08 de agosto de 2022**.

Por ser recente, o preço da **ARP nº 05/2021** dispensaria pesquisa de preços para comprovar a vantajosidade. Entretanto, com o fito de garantir segurança absoluta na escolha pela utilização da ARP já referida, será feita a comparação entre os preços encontrados.

Item 1 da ARP nº 05/2021- TRT13

Fonte de preços públicos	Quantidade de licenças	Valor unitário e prazo das licenças	Valor unitário proporcional para o período de 48 meses
TRF2 - JF-ES	1.100	R$ 112,00 - 36 meses	R$ 149,33
UFRGS	7.500	R$ 134,34 - 48 meses	R$ 134,34
TC-ES	700	R$ 213,87 - 36 meses	R$ 285,16
MP-MG	9.000	R$ 114,44 - 36 meses	R$ 152,59
TRT13	**82.809**	**R$ 125,60 - 48 meses**	**R$ 125,60**

Item 2 da ARP nº 05/2021- TRT13			
Fonte de preços públicos	**Quantidade de licenças**	**Valor unitário e prazo das licenças**	**Valor unitário proporcional para o período de 48 meses**
Senado Federal	150	R$ 152,160 - 12 meses	R$ 608,64
CRM-SC	150	R$ 88,00 - 12 meses	R$ 352,00
MP MT	2.500	R$ 103,00 - 36 meses	R$ 137,33
TRT13	**5.139**	**R$ 125,60 - 48 meses**	**R$ 125,60**

Da análise realizada, depreende-se que o preço das licenças do software de segurança dos endpoints na ARP nº 05/2021 do TRT13 é, além de recente, mais vantajoso que outros preços praticados em contratos públicos.

Se comparados com os preços privados, os preços das licenças ARP nº 05/2021 do TRT13 são também mais baratas. A única exceção é a proposta do fabricante Bitdefender que tem preço unitário mais barato. Contudo, como o serviço de desinstalação de solução em uso e instalação e configuração da sua própria ferramenta é bem mais cara, no total, a mudança para solução Bitdefender tem preço mais elevado.

Com relação aos serviços, a comparação se faz com os preços das propostas comerciais, já que nas contratações públicas acima analisadas esses serviços não aparecem, em função, em muitos casos, da manutenção da solução já em uso.

Itens 3 e 4 da ARP nº 05/2021- TRT13				
Fonte de preços	**Fabricante**	**Implantação e configuração da solução + Repasse de conhecimento hands-on**	**Treinamento EAD de capacitação técnica para administração da solução (por pessoa)**	**Total dos serviços**
M3TEC	Bitdefender	R$ 92.500,00	R$ 1.500,00	R$ 107.500,00
ENERGY TELECOM	SOPHOS	R$ 8.776,84	R$ 1.089,32	R$ 19.670,04
NETSAFE	Mcafee	R$ 15.000,00	R$ 5.000,00	R$ 65.000,00
ARP n° 05 - TRT13	**Kaspersky**	**R$ 16.000,00**	**R$ 2.600,00**	**R$ 42.000,00**

Confrontando-se os preços da ARP nº 05/2021 do TRT13 com os preços de mercado dos serviços de treinamento e instalação e configuração, verificou-se que os referidos preços estão dentro da faixa de preços praticados pelo mercado.

Vale ressaltar que os itens 3 e 4 estão associados diretamente ao fabricante especificado. Com isso, não há como contratar os itens 1 e 2 de um fabricante, e os itens 3 e 4 de outro. Dessa forma, a proposta da Energy Telecom, apesar de ter o menor preço para os itens 3 e 4, tem um valor muito mais elevado para os itens 1 e 2, R$ 418,80 e R$ 986,60 respectivamente.

Conclui-se, então, pela vantajosidade na utilização da ARP nº 05/2021 do TRT13.

1.4 Outras Soluções Disponíveis (Art. 14, II, a)

Todas as alternativas disponíveis para atender a presente demanda já foram analisadas no tópico 1.2.

1.4.1 Portal do Software Público Brasileiro (Art. 14, II, b)

Não há soluções existentes no Portal de Software Público Brasileiro que atendam essa demanda.

1.4.2 Alternativa no Mercado (Art. 14, II, c)

Todas as alternativas disponíveis já foram analisadas nos itens 1.2 e 1.4.

1.4.3 Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d)

Não se aplica.

1.4.4 Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e)

Não se aplica.

1.4.5 Modelo de Requisitos Moreq-Jus (Art. 14, II, f)

Não se aplica.

1.5 Análise dos Custos Totais da Demanda (Art. 14, III)

O custo total apresentado no item 1.8 contempla todo o valor necessário para atender a presente demanda.

Não há outros custos envolvidos.

1.6 Escolha e Justificativa da Solução (Art. 14, IV)

Considerando a análise feita no item 1.2, a aquisição de solução de segurança de endpoints e contratação de serviços associados é a única alternativa disponível para atender a demanda do TRT7.

1.6.1 Descrição da Solução (Art. 14, IV,a)

A demanda consiste na aquisição de licenças de software de segurança de endpoints com as características já explicitadas de forma resumida no item

1.2.1.2. e que atenda aos requisitos apresentados de forma detalhada ao longo dos itens 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6 e 1.1.7.

É importante considerar que a ARP nº 05/2021, da qual o TRT7 é co-participante, além de apresentar-se economicamente vantajosa para contratação, também oferece uma solução de segurança de endpoints do mesmo fabricante da atualmente em uso neste Tribunal. Esse fato elimina alguns riscos inerentes ao processo de mudança onde haja migração entre soluções de fabricantes distintos a citar: computadores que não respondem adequadamente à desinstalação e reinstalação e a falta de experiência e habitualidade no uso de nova ferramenta de software. Esses riscos são vencidos com o uso continuado, mas, durante o intervalo de tempo necessário para sua estabilização, expõe um pouco mais o ambiente computacional a um mundo repleto de ameaças virtuais, marca dos tempos atuais.

A contratação para atender a demanda em análise dar-se-á mediante utilização da ARP nº 05/2021 do TRT13, da qual o TRT7 é co-participante.

1.6.2 Alinhamento da Solução (Art. 14, IV, b)

A contratação está perfeitamente alinhada com a necessidade de manter a disponibilidade dos serviços de TIC e encontra-se alicerçada nos seguintes objetivos estratégicos do Planejamento Estratégico Institucional.

a) OBJETIVO DA PERSPECTIVA PROCESSOS INTERNOS – Fortalecer a Governança e a Gestão Estratégica : Aprimorar as estruturas de governança e gestão estratégica, de modo a desenvolver processos de trabalho inovadores, com suporte de sistemas digitais integrados de gestão de pessoal, de aquisições, de finanças, bem como os relacionados às atividades de compliance e gestão de riscos organizacional, que permitam a tramitação de processos e

documentos e a prática de atos de gestão com maior rastreabilidade, segurança**,** confiabilidade, integridade, atualidade, celeridade, transparência e eficiência. **PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL DO TRT7. (2021/2026)**

b) OBJETIVO DA PERSPECTIVA APRENDIZADO E CRESCIMENTO - Aprimorar a Governança de Tecnologia da informação e comunicação - TIC e a proteção de dados : Garantir o aprimoramento, a integridade e a disponibilidade dos sistemas de informação e dos bancos de dados mantidos pela Justiça do Trabalho, por meio de mecanismos de controle consistentes, bem como a modernização de ativos e tecnologias que visem à implementação de grandes bases de dados e aplicação de inteligência artificial para a melhoria dos processos de trabalho e da qualidade dos serviços prestados à sociedade.Alinhamento aos macrodesafios do Poder Judiciário: Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados. **PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL DO TRT7. (2021/2026)**

c) OBJETIVO 7: DA PERSPECTIVA PROCESSOS INTERNOS - Aprimorar a Segurança da Informação e a Gestão de Dados. Resolução nº 370, de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

O investimento encontra-se autorizado no Plano de Contratações de TIC de 2021, aprovado pelo Comitê de Governança de TIC. O item que indica a presente contratação no referido plano é “Solução de antivírus”.

1.6.3 Benefícios Esperados (Art. 14, IV, c)

Os benefícios advindos do atendimento à demanda que é objeto do presente estudo técnico preliminar serão os seguintes:

a. Atender às deliberações e aos atos oriundos do CSJT determinando a execução orçamentária dos itens orçamentários obrigatórios, entre os quais se incluem o antivírus;

b. Disponibilizar um ambiente computacional seguro minimizando os riscos quanto às ameaças eletrônicas, tais como vírus, worms, trojans, spywares, ransomwares;

c. Garantir a integridade e disponibilidade dos sistemas, principalmente PJe;

d. Reduzir os risco de que agentes maliciosos como vírus e outros propiciem a invasão do ambiente computacional do TRT7, provocando a comprometimento de informações ou roubo de dados;

e. Reduzir os riscos que um incidente de segurança de TI aconteça, prejudicando a reputação institucional do TRT7.

1.6.4 Relação entre a Demanda Prevista e a Contratada (Art. 14, IV, d)

As quantidades previstas para atender a demanda por solução de segurança de endpoints estão apresentadas abaixo.

ESTIMATIVA DE VOLUME DE SERVIÇOS OU BENS			
Item	**Descrição**	**Qtde**	**Forma de estimativa**

1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	2000	Quantidade de endpoints (desktops, notebooks e servidores de rede) em uso no Regional
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	200	Quantidade de máquinas virtuais
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	01	Quantidade necessária para fazer a implantação da nova solução, no caso de solução de fabricante diferente
4	Treinamento EAD de capacitação técnica para administração da solução	10	Quantidade de servidores que trabalham na unidade responsável pela operação e monitoramento da solução de segurança de endpoints, no caso de solução de fabricante diferente

1.7 Adequação do Ambiente (Art. 14, V, a, b, c, d, e, f)

Não há grande necessidade de adequações, considerando que o software a ser instalado é semelhante ao atualmente em uso neste Tribunal. No entanto, como a nova solução possui características que a antiga não detinha, pode ser necessário o aumento de recursos computacionais entregues para o produto, bem como a implantação de novas ferramentas de gerenciamento. De

forma geral, esses eventuais recursos adicionais podem ser acomodados nos equipamentos em uso no Datacenter do TRT7. Por sua vez, a implantação da solução faz parte do escopo da presente contratação.

1.8 Orçamento Estimado (Art. 14, II, g)

Os preços para a contratação, conforme valores constantes na ARP nº 05/2021 do TRT13, são os seguintes:

Item	Descrição	qtde	valor unitário	valor total	valor mensal do item (em 48 parcelas)
1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	2000	R$ 125,60	R$ 251.200,00	R$ 5.233,33
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	200	R$ 125,60	R$ 25.120,00	R$ 523,33
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	01	R$ 16.000,00	R$ 16.000,00	-

4	Treinamento EAD de capacitação técnica para administração da solução	10 (alunos)	R$ 2.600,00	R$ 26.000,00	-
			Total da contratação	R$ 318.320,00	

2. SUSTENTAÇÃO DO CONTRATO (Art.15)

2.1 Recursos Materiais e Humanos (Art. 15, I)

Para a contratação, não serão necessários recursos materiais e humanos adicionais. Os servidores da própria SETIC serão responsáveis pelo acompanhamento da entrega do software e dos serviços de instalação, configuração e treinamento, bem como pelas atividades relacionadas à fiscalização das obrigações da contratada ao longo da vigência do contrato.

Considerando que os serviços serão prestados de forma remota, os enlaces de Internet que o TRT7 dispõe serão suficientes para que o suporte seja prestado de forma adequada.

2.2 Estratégia de Continuidade Contratual (Art. 15, II)

A contratação terá vigência de 48 meses e, por isso, não haverá possibilidade de prorrogação por igual período.

Caso haja descontinuidade na prestação dos serviços de suporte e atualização por parte da contratada, as seguintes ações serão realizadas:

1. Aplicação das multas e sanções previstas em contrato, inclusive com eventual ressarcimento de perdas e danos;

2. Verificação com o fabricante acerca da disponibilização das atualizações e prestação de suporte padrão;

3. Início de processo para realização de nova contratação para o suporte com níveis de serviço de acordo com os padrões definidos neste estudo.

2.3 Transição Contratual e Encerramento (Art. 15, III, a, b, c, d, e)

Como se trata de serviço de caráter imprescindível, ao término da vigência do contrato (48 meses) deverá ser realizada nova licitação.

Haverá transferência de conhecimentos sobre a execução e a manutenção da solução contratada possibilitando a continuidade da operação por parte dos técnicos do TRT7.

Todos os eventuais acessos necessários aos colaboradores da contratada devem ser formalmente solicitados, contendo a descrição detalhada das funções que os seus funcionários executarão. Após o término das atividades, o contratante revogará todas as permissões concedidas durante o processo de implantação, exceto aquelas mandatórias para a execução de procedimentos de manutenções preventivas durante a vigência do contrato, o que deve ser formalmente solicitado e detalhado pela empresa contratada.

2.4 Estratégia de Independência Tecnológica (Art. 15, IV, a, b)

Por tratar-se de aquisição de software de oferta diversificada no mercado, a solução poderá ser substituída por outra ferramenta de outro fabricante a qualquer tempo, caso o suporte tenha problemas ao longo da

vigência estabelecida de 48 (quarenta e oito) meses. Obviamente, como já explicado ao longo deste documento, a mudança da solução de segurança de endpoint é algo trabalhoso. No entanto, não há caracterização de dependência tecnológica.

3. ESTRATÉGIA PARA A CONTRATAÇÃO(Art.16)

3.1 Natureza do Objeto (Art. 16, I)

a) Bens e serviços comuns de acordo com a Lei nº 10520/2002 e o Decreto nº 10.024/2019;

b) Trata-se da contratação de serviço continuado.

3.2 Necessidade dos serviços continuados

A solução contemplando o software de segurança dos endpoints será instalada de uma única vez. Contudo, o suporte e as atualizações do software deverão ser fornecidos ao longo de 48 meses para que se mantenha o parque computacional protegido de novas ameaças cibernéticas que venham a surgir.

3.3 Parcelamento do Objeto (Art. 16, II)

Não se aplica.

3.4 Adjudicação do Objeto (Art. 16, III)

Não se aplica.

3.5 Modalidade e Tipo de Licitação (Art. 16, IV)

Não se aplica.

3.6 Classificação e Indicação Orçamentária (Art. 16, V)

Item	Natureza da despesa
Licença de software de segurança para endpoints (estações de trabalho e servidores) + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	**33.90.40.11** - Suporte de Infraestrutura de TIC
Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por 48 meses.	**33.90.40.11** - Suporte de Infraestrutura de TIC
Implantação e configuração da solução + Repasse de conhecimento hands-on	**33.90.40.21** - Serviços técnicos de profissionais de TIC - PJ
Treinamento EAD de capacitação técnica para administração da solução.	**33.90.40.20** - Treinamento /capacitação em TIC

O investimento encontra-se autorizado pelo plano de contratações de 2021. A despesa decorrente desta contratação correrá à conta de recursos próprios do TRT7.

3.7 Vigência da Prestação de Serviço (Art. 16, VI)

A vigência do contrato será de 48 (quarenta e oito) meses, contados a partir da data de sua assinatura.

A justificativa para o prazo de 48 meses encontra-se no item **1.1.7.3.**

3.8 Equipe de Apoio à Contratação (Art. 16, VII)

Integrante técnico:

João Paulo Colares de Andrade.

Telefone: 3388-9314

E-mail: joaopaulo.andrade@trt7.jus.br

Integrante demandante:

Robson Teixeira da Silva.

Telefone: 3388-9201

E-mail: robson.teixeira@trt7.jus.br

Integrante administrativo:
Divânia Maria Alcântara Soares.

Telefone: 3388-9394

E-mail: divania@trt7.jus.br

3.9 Equipe de Gestão da Contratação (Art. 16, VIII)

Gestor do contrato:

Robson Teixeira da Silva.

Telefone: 3388-9201

E-mail: robson.teixeira@trt7.jus.br

Gestor substituto:

Roberto Paulo Dias Alcântara Filho.

Telefone: 3388-9201

E-mail: robertopdaf@trt7.jus.br

Fiscal técnico:

João Paulo Colares de Andrade.

Telefone: 3388-9314

E-mail: joaopaulo.andrade@trt7.jus.br

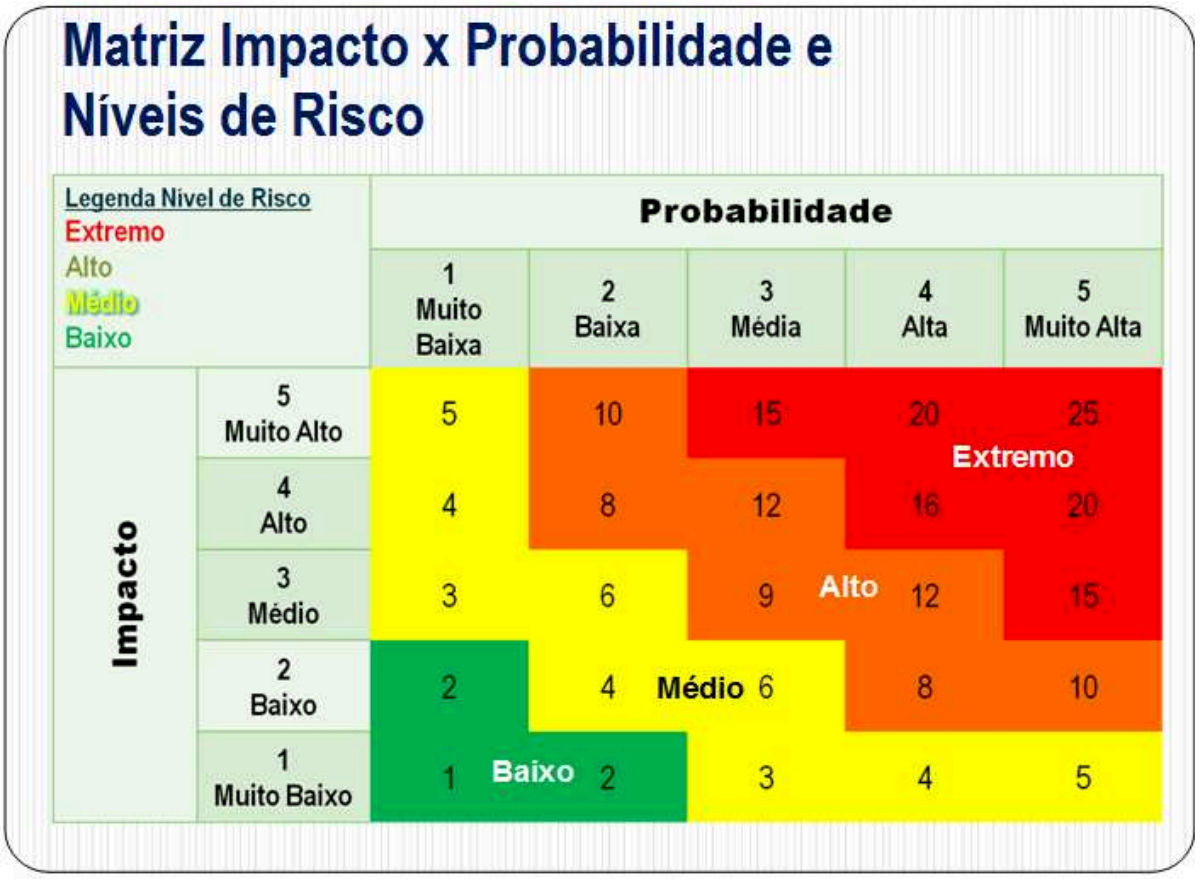
Fiscal substituto:

Fellyppe Carlos Santos de Lima.

Telefone: 3388-9314

E-mail: fellyppe@trt7.jus.br

4. ANÁLISE DE RISCOS



Risco 1	**Risco:**		**Identificação imprecisa da solução que atenda a demanda**	
	Probabilidade:	**Impacto:**	**Risco: (PxI)**	**Dano**
	1-Muito Baixa	4-Alto	4-Médio	Ocorrência de incidente de segurança com comprometimento da segurança dos ativos de TIC, podendo ocorrer indisponibilidade no PJe e demais aplicações.
	Ações de mitigação e de contingência			**Responsável**
	1 - Analisar as soluções possíveis e escolher a que melhor atenda a			Equipe de

	demanda do TRT7.	planejamento a contratação
	2 - Estabelecer novo estudo, caso necessário, ajustando eventuais necessidades de modo que a solução seja identificada.	Diretor da DITIC

Risco 2	**Risco:**		**Ausência de disponibilidade orçamentária**	
	Probabilidade:	**Impacto:**	**Risco: (PxI)**	**Dano**
	1-Baixa	3-Médio	3-Médio	A utilização da atual solução de segurança de endpoints sem atualização pode levar a incidentes de segurança da informação, podendo comprometer o desenvolvimento das atividades do Tribunal, em caso de incidentes graves.
	Ações de mitigação e de contingência			**Responsável**
	1 - Buscar nas soluções possíveis o princípio da economicidade.			Equipe de planejamento a contratação
	2 - Verificar junto a alta administração alternativas para continuidade do processo, tal como readequação orçamentária.			Diretor da DITIC

Risco 3	**Risco:**		**Atraso na contratação**	
	Probabilidade:	**Impacto:**	**Risco: (PxI)**	**Dano**
	1-Baixa	3-Médio	3-Médio	A utilização da atual solução de segurança de endpoints sem atualização pode levar a incidentes de segurança da informação, podendo comprometer o desenvolvimento das atividades do Tribunal, em caso de incidentes

				graves.
	Ações de mitigação e de contingência			**Responsável**
	1 - Iniciar com antecedência o planejamento da contratação.			Equipe de planejamento a contratação
	2 - Solicitar contratação emergencial da licença com validade extra da atual solução de segurança de endpoints até a nova contratação ser iniciada.			Diretor da DITIC

Risco 4	**Risco:**		**Falhas na prestação do serviço de suporte técnico**	
	Probabilidade:	**Impacto:**	**Risco: (PxI)**	**Dano**
	1-Muito Baixa	4-Alto	4-Médio	Utilização de software desatualizado ou demora na solução de falha de software que provoque indisponibilidade do antivírus, podendo dar causa a incidente de segurança com comprometimento da segurança dos ativos de TI, podendo comprometer o desenvolvimento das atividades do Tribunal.
	Ações de mitigação e de contingência			**Responsável**
	1 - Atuar diligentemente na fiscalização da execução contratual e exigir que a contratada cumpra suas obrigações.			Equipe de fiscalização da contratação
	2 - Solicitar a aplicação de eventuais penalidades. Iniciar um novo processo de contratação.			Diretor da DITIC

	Risco:		**Interrupção contratual por problemas com a empresa contratada.**

Risco 5	**Probabilidade:**	**Impacto:**	**Risco: (PxI)**	**Dano**
	1-Muito Baixa	4-Alto	4-Médio	Utilização de software desatualizado ou demora na solução de falha de software que provoque indisponibilidade do antivírus, podendo dar causa a incidente de segurança com comprometimento da segurança dos ativos de TIC, podendo comprometer o desenvolvimento das atividades do Tribunal.
	Ações de mitigação e de contingência			**Responsável**
	1 - Atuar diligentemente na fiscalização da execução contratual.			Equipe de fiscalização da contratação
	2 - Solicitar a aplicação de eventuais penalidades. Iniciar um novo processo de contratação.			Diretor da DITIC

5. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Considerando a demanda, a efetividade da solução, a capacidade de recepção do objeto, bem como seu armazenamento, distribuição e instalação, os integrantes da equipe de planejamento da contratação, descritos abaixo, declaram a viabilidade desta contratação.

6. ASSINATURAS

CIÊNCIA		
Integrante Técnico	**Integrante Requisitante**	**Integrante Administrativo**
_____ **João Paulo Colares de Andrade** **Mat.: 30871577**	_____ **Robson Teixeira da Silva** **Mat.:30871529**	_____ **Divânia Maria Alcântara Soares** **Mat.: 3087398**
Fortaleza, 25 de agosto de 2021.		

DE ACORDO
Diretor da Secretaria de Tecnologia da Informação e Comunicação
_____ **Francisco Jonathan Rebouças Maia** **Mat.: 30871392**
Fortaleza, 26 de agosto de 2021.