PROCESSO Nº 26.856/2022-TJMA
CONTRATO Nº 0034/2023-TJMA
PREGÃO ELETRÔNICO 0008/2023-TJMA
ARP Nº 0019/2023-TJMA

CONTRATO DE PRESTAÇÃO DE SERVIÇO QUE ENTRE SI CELEBRAM O TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO E A EMPRESA NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.

O TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO, órgão do Poder Judiciário, inscrito no CNPJ sob o n.º 05.288.790/0001–76, com sede na Av. Dom Pedro II, s/nº, Palácio "Clovis Bevilácqua", Centro, CEP: 65.010-905, São Luís/MA, representado pelo seu Presidente, o **Desembargador PAULO SÉRGIO VELTEN PEREIRA**, brasileiro, residente e domiciliado nesta cidade, inscrito no CPF sob o n° 257.545.483-20, portador da carteira de identidade RG nº 926.136 SSP/MA, doravante denominado **CONTRATANTE,** e de outro a **EMPRESA NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA ,** CNPJ Nº 05.250.796/0001-54 , sediada à Av. Pontes Vieira, 2340 - Dionisio Torres, UNO - Medical & Office - Sala 510 à 514 - 5º andar, CEP: 60135-238, Fortaleza-CE, Telefone: (85)3195-2200/2231/2212, E-mail: yure.sabino@networksecure.com.br/licitacoes@networksecure.com.br, neste ato representada pelo **Sr**. **YURE LEOPOLDO SABINO DE FREITAS**, inscrita no CPF sob o nº 525.285.023-20, doravante denominada **CONTRATADA**, e em observância às disposições da Lei nº 10.520, de 17 de julho de 2002, subsidiariamente à Lei nº 8.666/93, de 21 de junho de 1993, mediante cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – DO OBJETO DO CONTRATO

1.1 Constitui objeto do presente a contratação de empresa especializada para a renovação das licenças de uso de software antivírus com upgrade do Kaspersky Endpoint Security for Business ADVANCED, incluindo suporte técnico remoto**,**

Item 01

Descrição	Quantidade total R$	Valor unitário R$
Fornecimento da renovação de licenças de uso do software de antivírus Kaspersky Endpoint Security For Business com upgrade para ADVANCED, com suporte técnico, por 03 anos.	8.000	143,00
Valor total: R$ 1.144.000,00 (Um Milhão, Cento e Quarenta e Quatro Mil Reais)		

1.2.1 Requisitos técnicos

1.2.1.1 Suporte técnico e garantia do fabricante ou empresa devidamente credenciada e autorizada;

1.2.1.2 Suporte especializado a ser prestado na modalidade *on-site* (quando necessário), nas dependências do respectivo órgão **CONTRATANTE**, sem prejuízo ao atendimento via remoto/telefone;

1.2.1.3 Proteção de todos os equipamentos, atuais e novos a serem adquiridos, contra softwares indesejados;

1.2.1.4 Impedir a disseminação e proliferação de ameaças virtuais;

1.2.2 Características Técnicas mínimas a serem atendidas:

1.2.2.1 Servidor de Administração e Console Administrativa

1.2.2.1.1 **Compatibilidade:**

1.2.2.1.1.1 Microsoft Windows Server 2012/R2 (Todas as edições);

1.2.2.1.1.2 Microsoft Windows Server 2016 x64;

1.2.2.1.1.3 Microsoft Windows 8 SP1 Professional / Enterprise x86/x64;

1.2.2.1.1.4 Microsoft Windows 8/8.1 Professional / Enterprise X86/x64;

1.2.2.1.1.5 Microsoft Windows 10 (Todas as edições);

1.2.2.1.1.6 Microsoft Windows 11;

1.2.2.2 Suporta as seguintes plataformas virtuais:

1.2.2.2.1 Vmware: Workstation 16.x Pro, vSphere 6.7, vSphere 7;

1.2.2.2.2 Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64;

1.2.2.2.3 Citrix XenServer 7.1 LTSR e 8;

1.2.2.3 Características:

1.2.2.3.1 Console deve ser acessada via WEB (HTTPS) ou MMC;

1.2.2.3.2 Console deve ser baseada no modelo cliente/servidor;

1.2.2.3.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

1.2.2.3.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

1.2.2.3.5 Deve permitir incluir usuários do AD para logarem na console de administração;

1.2.2.3.6 Console deve ser totalmente integrada com as suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

1.2.2.3.7 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

1.2.2.3.8 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

1.2.2.3.9 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
1.2.2.3.10 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.2.2.3.11 Deve armazenar histórico das alterações feitas em políticas;
1.2.2.3.12 Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
1.2.2.3.13 Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
1.2.2.3.14 A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.2.2.3.15 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.2.2.3.16 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
1.2.2.3.17 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.2.2.3.18 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os parâmetros KB/s e horário;
1.2.2.3.19 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução;
1.2.2.3.20 Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
1.2.2.3.21 Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
1.2.2.3.22 Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;
1.2.2.3.23 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
1.2.2.3.24 Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
1.2.2.3.25 A comunicação entre o cliente e o servidor de administração deve ser criptografada;
1.2.2.3.26 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
1.2.2.3.27 Capacidade de aplicar atualizações do Windows remotamente nas estações e servidores;
1.2.2.3.28 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

1.2.2.3.29 Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
1.2.2.3.30 Capacidade de monitorar diferentes subredes a fim de encontrar máquinas novas para serem adicionadas à proteção;
1.2.2.3.31 Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas à proteção;
1.2.2.3.32 Capacidade de, assim que detectar máquinas novas no Active Directory, subredes ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
1.2.2.3.33 Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos dois dias, etc.;
1.2.2.3.34 Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
1.2.2.3.35. Deve fornecer as seguintes informações dos computadores: Se o antivírus está instalado; Se o antivírus está iniciado; Se o antivírus está atualizado; Minutos/horas desde a última conexão da máquina com o servidor administrativo; Minutos/horas desde a última atualização de vacinas; Data e horário da última verificação executada na máquina; Se é necessário reiniciar o computador para aplicar mudanças; Data e horário de quando a máquina foi ligada; Quantidade de vírus encontrados (contador) na máquina; Nome do computador; Domínio ou grupo de trabalho do computador; Data e horário da última atualização de vacinas; Sistema operacional com Service Pack; Quantidade de processadores; Quantidade de memória RAM; Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory); Endereço IP; Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido; Atualizações do Windows Updates instaladas; Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD; Vulnerabilidades de aplicativos instalados na máquina;
1.2.2.3.36 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.2.2.3.37 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como: Alteração de Gateway Padrão; Alteração de subrede; Alteração de domínio; Alteração de servidor DHCP; Alteração de servidor DNS; Resolução de Nome; Disponibilidade de endereço de conexão SSL;

1.2.2.3.38 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.2.2.3.39 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
1.2.2.3.40 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.2.2.3.41 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.2.2.3.42 Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
1.2.2.3.43 Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
1.2.2.3.44 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
1.2.2.3.45 Capacidade de gerar traps SNMP para monitoramento de eventos;
1.2.2.3.46 Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.2.2.3.47 Listar em um único local, todos os computadores não gerenciados na rede;
1.2.2.3.48 Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
1.2.2.3.49 Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
1.2.2.3.50 Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
1.2.2.3.51 Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
1.2.2.3.52 Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subredes diferentes do servidor;
1.2.2.3.53 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.2.2.3.54 Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos a outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
1.2.2.3.55 Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex.: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

1.2.2.3.56 Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
1.2.2.3.57 Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
1.2.2.3.58 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
1.2.2.3.59 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo: Nome do vírus; Nome do arquivo infectado; Data e hora da detecção; Nome da máquina ou endereço IP; Ação realizada;
1.2.2.3.60 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
1.2.2.3.61 Capacidade de listar updates nas máquinas com o respectivo link para download
1.2.2.3.62 Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
1.2.2.3.63 Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
1.2.2.3.64 Capacidade de realizar inventário de hardware de todas as máquinas clientes;
1.2.2.3.65 Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
1.2.2.3.66 Capacidade de diferenciar máquinas virtuais de máquinas físicas.

1.2.3. Estações Windows
1.2.3.1 Compatibilidade:
1.2.3.1.1 Microsoft Windows 8 Professional/Enterprise x86 /x64;
1.2.3.1.2 Microsoft Windows 8.1 Pro / Enterprise x86 /x64;
1.2.3.1.3 Microsoft Windows 10 Pro / Enterprise x86 /x64;
1.2.3.1.4 Microsoft Windows Server 2012 R2 Standard x64;
1.2.3.1.5 Microsoft Windows Server 2012 Foundation x64;
1.2.3.1.6 Microsoft Windows Server 2012 Standard x64;
1.2.3.1.7 Microsoft Small Business Server 2011 Standard x64;
1.2.3.1.8 Microsoft Windows Server 2016 x64;
1.2.3.1.9 Microsoft Windows 11.
1.2.3.2 Características:
1.2.3.2.1 Deve prover as seguintes proteções:
1.2.3.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
1.2.3.2.1.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

1.2.3.2.1.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
1.2.3.2.1.4 Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc.);
1.2.3.2.1.5 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
1.2.3.2.1.6 Firewall com IDS;
1.2.3.2.1.7 Autoproteção (contra-ataques aos serviços/processos do antivírus);
1.2.3.2.1.8 Controle de dispositivos externos;
1.2.3.2.1.9 Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
1.2.3.2.1.10 Controle de acesso a sites por horário;
1.2.3.2.1.11 Controle de acesso a sites por usuários;
1.2.3.2.1.12 Controle de acesso a websites por dados, ex.: Bloquear websites com conteúdos de vídeo e áudio;
1.2.3.2.1.13 Controle de execução de aplicativos;
1.2.3.2.1.14 Controle de vulnerabilidades do Windows e dos aplicativos instalados;
1.2.3.2.2 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
1.2.3.2.3 As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, **no máximo, uma em uma hora** independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
1.2.3.2.4 Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;
1.2.3.2.5 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
1.2.3.2.6 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex.: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
1.2.3.2.7 Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
1.2.3.2.8 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
1.2.3.2.9 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
1.2.3.2.10 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

1.2.3.2.11 Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
1.2.3.2.12 Capacidade de verificar somente arquivos novos e alterados;
1.2.3.2.13 Capacidade de verificar objetos usando heurística utilizando no mínimo as seguintes opções de nível: Alta, Média, Baixa;
1.2.3.2.14 Capacidade de agendar uma pausa na verificação;
1.2.3.2.15 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
1.2.3.2.16. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
1.2.3.2.17 Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
1.2.3.2.18 Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
1.2.3.2.19 Capacidade de verificar links inseridos em e-mails contra phishings;
1.2.3.2.20 Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
1.2.3.2.21 Capacidade de verificação de corpo e anexos de e-mails usando heurística;
1.2.3.2.22 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
1.2.3.2.23 Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
1.2.3.2.24 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
1.2.3.2.25 Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
1.2.3.2.26 Deve ter suporte total ao protocolo Ipv6;
1.2.3.2.27 Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
1.2.3.2.28 Na verificação de tráfego web, caso encontrado código malicioso o programa deve: Perguntar o que fazer, ou Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou Permitir acesso ao objeto;
1.2.3.2.29 O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador: Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;
1.2.3.2.30 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
1.2.3.2.31 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;

1.2.3.2.32 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
1.2.3.2.33 Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
1.2.3.2.34 Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);
1.2.3.2.35 Capacidade de distinguir diferentes subredes e conceder opção de ativar ou não o firewall para uma subrede específica;
1.2.3.2.36 Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
1.2.3.2.37 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; Filtragem por aplicativo onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;
1.2.3.2.38 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo: Discos de armazenamento locais; Armazenamento removível; Impressoras; CD/DVD; Modems; Dispositivos de fita; Dispositivos multifuncionais; Leitores de smart card; Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc); Wi-Fi; Adaptadores de rede externos; Dispositivos MP3 ou smartphones; Dispositivos Bluetooth; Câmeras e Scanners.
1.2.3.2.39 Capacidade de liberar acesso a um dispositivo específico e usuários específico por um período de tempo específico, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
1.2.3.2.40 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
1.2.3.2.41 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
1.2.3.2.42 Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
1.2.3.2.43 Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
1.2.3.2.44 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento.
1.2.3.2.45 Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo,

fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
1.2.3.2.46 O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação: Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
1.2.3.2.47 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
1.2.3.2.48 Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
1.2.3.2.49 Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
1.2.3.2.50 Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
1.2.3.2.51 Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
1.2.3.2.52 Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
1.2.3.2.53 Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
1.2.3.2.54 Capacidade de integração com o Windows Defender Security Center.
1.2.3.2.55 Capacidade de integração com a Antimalware Scan Interface (AMSI).
1.2.3.2.56 Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).
1.2.3.2.57 Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.

1.2.4 Estações Mac OS X
1.2.4.1 Compatibilidade:
1.2.4.1.1 MacOS High Sierra 10.13
1.2.4.1.2 MacOS Sierra 10.12
1.2.4.1.3 Mac OS X 10.11 (El Capitan);
1.2.4.1.4 Mac OS X 10.10 (Yosemite);
1.2.4.1.5 Mac OS X 10.9 (Mavericks);
1.2.4.2 Características:
1.2.4.2.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

1.2.4.2.2 Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;
1.2.4.2.3 Possuir módulo de bloqueio á ataques na rede;
1.2.4.2.4 Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
1.2.4.2.5 Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio a ataques na rede;
1.2.4.2.6 Possibilidade de importar uma chave no pacote de instalação;
1.2.4.2.7 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
1.2.4.2.8 Deve possuir suportes a notificações utilizando o Growl;
1.2.4.2.9 As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
1.2.4.2.10 Capacidade de voltar para a base de dados de vacina anterior;
1.2.4.2.11 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
1.2.4.2.12 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex.: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
1.2.4.2.13 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
1.2.4.2.14 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.2.4.2.15 Capacidade de verificar somente arquivos novos e alterados;
1.2.4.2.16 Capacidade de verificar objetos usando heurística;
1.2.4.2.17 Capacidade de agendar uma pausa na verificação;
1.2.4.2.18 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer ou Bloquear acesso ao objeto ou Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
1.2.4.2.18.1 Caso positivo de desinfecção restaurar o objeto para uso;
1.2.4.2.18.2 Caso negativo de desinfecção Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);
1.2.4.2.19 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
1.2.4.2.20 Capacidade de verificar arquivos de formato de e-mail;
1.2.4.2.21 Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

1.2.4.2.22 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

1.2.5 Estações de trabalho Linux 32-64 bits

1.2.5.1 Compatibilidade:

1.2.51.1 Ubuntu 18.04, 20.04
1.2.5.1.2 Red Hat® Enterprise Linux® 6.9
1.2.5.1.3 CentOS-6.9
1.2.5.1.4 Debian GNU/Linux 9.4, 10.1, 11.1
1.2.5.1.5 AltLinux 8.0.0
1.2.5.1.6 AltLinux 8.2
1.2.5.1.7 GosLinux 6.6
1.2.5.1.8 Red Hat® Enterprise Linux® 7.4
1.2.5.1.9 CentOS-7.4
1.2.5.1.10 OracleLinux 7.4
1.2.5.1.11 SUSE® Linux Enterprise Server 12 SP5
1.2.5.1.12 OpenSUSE® 42.3
1.2.5.1.13 AltLinux 8.0.0

1.2.5.2 Características:

1.2.5.2.1 Deve prover as seguintes proteções:
1.2.5.2.2 Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.2.5.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, **no máximo, uma em uma hora** independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
1.2.5.2.4 Capacidade de configurar a permissão de acesso às funções do antivírus;
1.2.5.2.5 Capacidade de criar exclusões por local, máscara e nome da ameaça;
1.2.5.2.6 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
1.2.5.2.7 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
1.2.5.2.8 Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
1.2.5.2.9 Capacidade de verificar objetos usando heurística utilizando no mínimo as seguintes opções de nível: Alta, Média, Baixa;
1.2.5.2.10. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
1.2.5.2.11 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

1.2.5.2.12 Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
1.2.5.2.13 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
1.2.5.2.14 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.2.5.2.15 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
1.2.5.2.16 Administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

1.2.6 Servidores Windows 32 ou 64 bits
1.2.6.1 Compatibilidade:
1.2.6.1.1 Microsoft Windows Storage Server SP2 Workgroup Edition;
1.2.6.1.2 Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
1.2.6.1.3 Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
1.2.6.1.4 Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
1.2.6.1.5 Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
1.2.6.1.6 Microsoft Windows Storage Server 2012 (Todas edições);
1.2.6.1.7 Microsoft Windows Storage Server 2012 R2 (Todas edições);
1.2.6.1.8 Microsoft Windows Hyper-V Server 2012;
1.2.6.1.9 Microsoft Windows Hyper-V Server 2012 R2;
1.2.6.1.10 Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server;
1.2.6.1.11 Windows Server 2016 Core Standard / Datacenter;
1.2.6.1.12 Windows Storage Server 2016;
1.2.6.1.13 Windows Hyper-V Server 2016.
1.2.6.2 Características:
1.2.6.2.1 Deve prover as seguintes proteções:
1.2.6.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
1.2.6.2.1.2 Auto-proteção contra-ataques aos serviços/processos do antivírus;
1.2.6.2.1.3 Firewall com IDS;
1.2.6.2.1.4 Controle de vulnerabilidades do Windows e dos aplicativos instalados;
1.2.6.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

1.2.6.2.3 As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, **no máximo, uma em uma hora** independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
1.2.6.2.4 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); Gerenciamento de tarefa (criar ou excluir tarefas de verificação); Leitura de configurações; Modificação de configurações; Gerenciamento de Backup e Quarentena; Visualização de relatórios; Gerenciamento de relatórios; Gerenciamento de chaves de licença; Gerenciamento de permissões (adicionar/excluir permissões acima);
1.2.6.2.5 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo, terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
1.2.6.2.6 Capacidade de separadamente selecionar o número de processos que executarão funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
1.2.6.2.7 Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede
1.2.6.2.8 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
1.2.6.2.9 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja rodando com fonte ininterrupta de energia (*uninterruptible Power supply – UPS*);
1.2.6.2.10 Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
1.2.6.2.11 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
1.2.6.2.12 Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
1.2.6.2.13 Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
1.2.6.2.14 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
1.2.6.2.15 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

1.2.6.2.16 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
1.2.6.2.17 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.2.6.2.18 Capacidade de verificar somente arquivos novos e alterados;
1.2.6.2.19 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
1.2.6.2.20 Capacidade de verificar objetos usando heurística;
1.2.6.2.21 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
1.2.6.2.22 Capacidade de agendar uma pausa na verificação;
1.2.6.2.23 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
1.2.6.2.24 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer ou Bloquear acesso ao objeto; Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
1.2.6.2.24.1 Caso positivo de desinfecção restaurar o objeto para uso;
1.2.6.2.24.2 Caso negativo de desinfecção mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);
1.2.6.2.25 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
1.2.6.2.26 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
1.2.6.2.27 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
1.2.6.2.28 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;
1.2.6.2.29 Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros
1.2.6.2.30 Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);
1.2.6.2.31 Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

1.2.7 Servidores Linux 32 ou 64 bits
1.2.7.1 Compatibilidade:
1.2.7.1.1 Red Hat® Enterprise Linux® 6.9 Server
1.2.7.1.2 CentOS-6.9
1.2.7.1.3 Ubuntu 18.04, 20.04

1.2.7.1.4 Debian GNU / Linux 9.4, 10.1, 11.1
1.2.7.1.5 AltLinux 8.0.0
1.2.7.1.6 AltLinux 8.2
1.2.7.1.7 Red Hat® Enterprise Linux® 7.4 Server
1.2.7.1.8 Red Hat® Enterprise Linux® 7.5 Server
1.2.7.1.9 CentOS-7.4
1.2.7.1.10 CentOS-7.5
1.2.7.1.11 Ubuntu 18.04
1.2.7.1.12 SUSE® Linux Enterprise Server 12 SP5
1.2.7.1.13 Oracle Linux 7.4
1.2.7.1.14 SUSE® Linux Enterprise Server 12 SP2
1.2.7.1.15 OpenSUSE® 42.3
1.2.7.1.16 Amazon Linux 2

1.2.7.2 Características:

1.2.7.2.1 Deve prover as proteções de Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.2.7.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
1.2.7.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar tarefas);
1.2.7.2.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
1.2.7.2.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
1.2.7.2.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
1.2.7.2.3 Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
1.2.7.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
1.2.7.2.5 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção;
1.2.7.2.6 Capacidade de verificar objetos usando heurística;
1.2.7.2.7 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
1.2.7.2.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
1.2.7.2.9 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

1.2.8 Smartphones e tablets

1.2.8.1 Compatibilidade:

1.2.8.1.1 Dispositivos com os sistemas operacionais:

1.2.8.1.1.1 Android 5.0 – 5.1.1 ou superior

1.2.8.1.1.2 iOS 9.0 – 9.3.5 ou superior

1.2.8.2 Características:

1.2.8.2.1 Deve prover as seguintes proteções:

1.2.8.2.1.1 Proteção em tempo real do sistema de arquivos do dispositivo;

1.2.8.2.1.2 Proteção contra adware e autodialers;

1.2.8.2.1.3 Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

1.2.8.2.1.4 Arquivos abertos no smartphone;

1.2.8.2.1.5 Programas instalados usando a interface do smartphone

1.2.8.2.1.6 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

1.2.8.2.2 Deverá isolar em área de quarentena os arquivos infectados;

1.2.8.2.3 Deverá atualizar as bases de vacinas de modo agendado;

1.2.8.2.4 Deverá bloquear spams de SMS através de Black lists;

1.2.8.2.5 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;

1.2.8.2.6 Capacidade de desativar por política: Wi-fi; Câmera; Bluetooth.

1.2.8.2.7 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

1.2.8.2.8 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

1.2.8.2.9 Deverá ter firewall pessoal (Android);

1.2.8.2.10 Capacidade de tirar fotos quando a senha for inserida incorretamente;

1.2.8.2.11 Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

1.2.8.2.12 Capacidade de enviar comandos remotamente de: Localizar; Bloquear.

1.2.8.2.13 Capacidade de detectar Jailbreak em dispositivos iOS;

1.2.8.2.14 Capacidade de bloquear o acesso a site por categoria em dispositivos;

1.2.8.2.15 Capacidade de bloquear o acesso a sites phishing ou malicioso;

1.2.8.2.16 Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;

1.2.8.2.17 Capacidade de configurar White e blacklist de aplicativos;

1.2.8.2.18 Capacidade de localizar o dispositivo quando necessário;

1.2.8.2.19 Permitir atualização das definições quando estiver em “roaming”;

1.2.8.2.20 Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

1.2.8.2.21 Deve permitir verificar somente arquivos executáveis;

1.2.8.2.22. Deve ter a capacidade de desinfectar o arquivo se possível;
1.2.8.2.23 Capacidade de agendar uma verificação;
1.2.8.2.24 Capacidade de enviar URL de instalação por e-mail;
1.2.8.2.25 Capacidade de fazer a instalação através de um link QRCode;
1.2.8.2.26 Capacidade de executar as seguintes ações caso a desinfecção falhe: Deletar; Ignorar; Quarentenar; Perguntar ao usuário.

1.2.9 Gerenciamento de dispositivos móveis (MDM)
1.2.9.1 Compatibilidade:
1.2.9.1.1 Dispositivos com os sistemas operacionais:
1.2.9.1.1.1 Android 5.0 – 5.1.1 ou superior
1.2.9.1.1.2 iOS 9.0 – 9.3.5 ou superior
1.2.9.1.2 Softwares de gerência de dispositivos:
1.2.9.1.2.1 Kaspersky Security Center 10 SP2 MR1 e superior;
1.2.9.1.2.2 Kaspersky Endpoint Security Cloud 3.0 e superior;
1.2.9.1.2.3 VMWare AirWatch 9.2 e superior;
1.2.9.1.2.4 MobileIron 9.6 e superior;
1.2.9.1.2.5 IBM Maas360 10.66 e superior;
1.2.9.1.2.6 SOTI MobiControl 14.1.0 (1152) e superior;
1.2.9.2 Características:
1.2.9.2.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
1.2.9.2.2 Capacidade de ajustar as configurações de: sincronização de e-mail; uso de aplicativos; senha do usuário; criptografia de dados; conexão de mídia removível.
1.2.9.2.3 Capacidade de instalar certificados digitais em dispositivos móveis;
1.2.9.2.4 Capacidade de, remotamente, resetar a senha de dispositivos iOS;
1.2.9.2.5 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
1.2.9.2.6 Capacidade de, remotamente, bloquear um dispositivo iOS;
1.2.9.2.7 Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
1.2.9.2.8 Permitir sincronização com perfil do “Touch Down”;
1.2.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo;
1.2.9.2.10 Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
1.2.9.2.11 Capacidade de sincronizar com Samsung Knox;
1.2.9.2.12 Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

1.2.10 Criptografia
1.2.10.1 Compatibilidade
1.2.10.1.1 Microsoft Windows 8/8.1 Enterprise/Pro x86/x64;

1.2.10.1.2 Microsoft Windows 10 Enterprise x86/x64;

1.2.10.1.3 Microsoft Windows 10 Pro x86/x64;
1.2.10.1.4 Microsoft Windows 11;

1.2.10.2 Características

1.2.10.2.1 O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
1.2.10.2.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
1.2.10.2.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
1.2.10.2.4 Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;
1.2.10.2.5 Permitir criar vários usuários de autenticação pré-boot;
1.2.10.2.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
1.2.10.2.7 Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
1.2.10.2.7.1 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
1.2.10.2.7.2 Criptografar todos os arquivos individualmente;
1.2.10.2.7.3 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
1.2.10.2.7.4 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
1.2.10.2.8 Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
1.2.10.2.9 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
1.2.10.2.10 Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
1.2.10.2.11 Verificar compatibilidade de hardware antes de aplicar a criptografia;
1.2.10.2.12 Possibilita estabelecer parâmetros para a senha de criptografia;
1.2.10.2.13 Bloqueia o reuso de senhas;
1.2.10.2.14 Bloqueia a senha após um número de tentativas pré-estabelecidas;
1.2.10.2.15 Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
1.2.10.2.16 Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

1.2.10.2.17 Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

1.2.10.2.18 Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
1.2.10.2.19 Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc;
1.2.10.2.20 Permite criar um grupo de extensões de arquivos a serem criptografados;
1.2.10.2.21 Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
1.2.10.2.22 Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
1.2.10.2.23 Capacidade de deletar arquivos de forma segura após a criptografia;
1.2.10.2.24 Capacidade de criptografar somente o espaço em disco utilizado;
1.2.10.2.25 Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
1.2.10.2.26 Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
1.2.10.2.27 Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
1.2.10.2.28 Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
1.2.10.2.29 Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
1.2.10.2.30 Capacidade de fazer “Hardware encryption”.

1.2.11 Gerenciamento de Sistemas
1.2.11.1 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;
1.2.11.2 Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
1.2.11.3 Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
1.2.11.4 Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
1.2.11.5 Capacidade de gerenciar licenças de softwares de terceiros;
1.2.11.6 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
1.2.11.7 Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, etc);
1.2.11.8 Possibilita fazer distribuição de software de forma manual e agendada;
1.2.11.9 Suporta modo de instalação silenciosa;

1.2.11.10 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
1.2.11.11 Possibilita fazer a distribuição através de agentes de atualização;
1.2.11.12 Utiliza tecnologia multicast para evitar tráfego na rede;
1.2.11.13 Possibilita criar um inventário centralizado de imagens;
1.2.11.14 Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
1.2.11.15 Suporte a WakeOnLan para deploy de imagens;
1.2.11.16 Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
1.2.11.17 Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
1.2.11.18 Capacidade de gerar relatórios de vulnerabilidades e patches;
1.2.11.19 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
1.2.11.20 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
1.2.11.21 Permite baixar atualizações para o computador sem efetuar a instalação;
1.2.11.22 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
1.2.11.23 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
1.2.11.24 Permite selecionar produtos a serem atualizados pela console de gerenciamento;
1.2.11.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
1.2.11.26 Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
1.2.11.27 Capacidade de instalar atualizações ou correções somente em computadores definidos ou em grupos definidos conforme selecionado pelo administrador;
1.2.11.28 Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
1.2.11.29 Deve permitir selecionar o idioma das aplicações que serão atualizadas;
1.2.11.30 Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;
1.2.11.30.1 Capacidade de definir listas de tipos de objetos que não serão verificados;
1.2.11.30.2 Capacidade de definir listas de servidores que não terão o tráfego verificado;
1.2.11.30.3 Capacidade de definir grupos de usuários e aplicar regras de verificação por grupos.

CLÁUSULA SEGUNDA – DA VIGÊNCIA

2.1 O Contrato terá a vigência de 36 (trinta e seis) meses, contados a partir da data de sua assinatura, prorrogável na forma do art. 57, inc. II, da Lei 8.666/93.

CLÁUSULA TERCEIRA – DO VALOR

3.1 O valor total deste Contrato é de R$ 1.144.000,00 (Um Milhão, Cento e Quarenta e Quatro Mil Reais), incluído no mesmo todas as despesas e custos, diretos e indiretos, incidentes sobre o objeto fornecido.

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1 Os recursos orçamentários para atender ao pagamento do objeto deste Contrato correrão à Dotação Orçamentária seguinte:
UNIDADE ORÇAMENTÁRIA: 04901 – FUNDO ESPECIAL DE MODERNIZAÇÃO E REAPARELHAMENTO DO JUDICIÁRIO – FERJ; FUNÇÃO: 02 – JUDICIÁRIA; PROGRAMA: 0543 – PRESTAÇÃO JURISDICIONAL; AÇÃO ORÇAMENTÁRIA: 4436 MODERNIZAÇÃO DO JUDICIÁRIO; NATUREZA DE DESPESA: 339040 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

4.2 A Nota fiscal deverá ser emitida em nome do FUNDO ESPECIAL DE MODERNIZAÇÃO E REAPARELHAMENTO DO JUDICIÁRIO – FERJ, CNPJ: 04.408.070/0001-34.

CLÁUSULA QUINTA – DAS CONDIÇÕES DE PAGAMENTO

5.1 O Tribunal de Justiça do Estado do Maranhão realizará o pagamento no prazo de até 30 (trinta) dias, contado do recebimento definitivo dos produtos;
5.2. O pagamento será efetuado mediante crédito na conta-corrente da **CONTRATADA** por Ordem Bancária, no prazo não superior a 30 (trinta) dias, conforme disposto no art.40, XIV, “a”, da Lei nº 8.666/93, quando mantidas as mesmas condições iniciais de habilitação e caso não haja fato impeditivo para o qual não tenha concorrido.
5.3 A **CONTRATADA** deverá encaminhar junto à nota fiscal documentos de regularidade para com as fazendas Federal, Estadual e Municipal; relativa à Seguridade Social; regularidade do FGTS e da Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela justiça do Trabalho;
5.3.1 Se durante a análise da documentação apresentada juntamente com a Nota Fiscal, o Fiscal verificar a falta de documento ou a necessidade de algum esclarecimento por parte da **CONTRATADA**, o notificará para que corrija a pendência ou preste o devido esclarecimento, no prazo de 48hs;
5.3.2 A partir da notificação, o prazo para pagamento será suspenso até que a **CONTRATADA** diligencie para solução da pendência;

5.3.3. Caso a licitante vencedora não faça as correções apontadas no prazo de 48 (quarenta e oito) horas, incidirá nas sanções previstas na cláusula de Sanções e Penalidades
5.4 A devolução da documentação de cobrança não aprovada pelo TJMA não servirá de motivo para que a **CONTRATADA** suspenda a execução de serviços;
5.5 Nenhum pagamento será efetuado enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.
5.6 A nota fiscal apresentada com erro será devolvida à **CONTRATADA** para retificação e reapresentação, acrescentando-se no prazo aqui fixado os dias que se passarem entre a data da devolução e a da reapresentação;

5.7 A data de vencimento da fatura nunca poderá ser inferior a 30 dias da data de seu efetivo encaminhamento ao Tribunal de Justiça;
5.8 Havendo penalidade de multa, glosas ou indenizações, o valor poderá ser deduzido do crédito que a **CONTRATADA** porventura fizer jus;
5.9 A nota fiscal deve conter as seguintes especificações: a data de emissão da nota fiscal, o valor unitário e total, de acordo com a proposta apresentada, número da conta bancária da empresa, nome do banco e respectiva agência, para recebimento dos créditos e número do referido empenho.
5.10 O CNPJ constante da nota fiscal deverá ser o mesmo na nota de empenho e vinculado à conta-corrente da **CONTRATADA**.
5.11 Os valores dos tributos incidentes sobre o fornecimento ora contratado deverão ser destacados na respectiva nota fiscal e/ou fatura, sempre que a legislação tributária o permitir, sendo certo que, no preço ajustado, já estarão inclusos os valores dos referidos tributos;
5.12 O TJMA só autorizará a realização do pagamento, se houver o ATESTE comprovando que o objeto atende às especificações técnicas e exigências descritas no Termo de Referência e demais determinações previstas no edital da licitação e na legislação de regência.
5.13 Na eventualidade de a vencedora decidir efetuar o faturamento por meio de CNPJ (matriz ou filial) distinto do constante da nota de empenho, deverá comprovar a regularidade fiscal tanto do estabelecimento contratado como do estabelecimento que efetivamente executar o objeto, por ocasião dos pagamentos.
5.13.1 Para faturamento conforme acima a empresa deverá manifestar sua intenção antes da autorização da contratação e empenho do objeto;
5.14 A **CONTRATADA** deverá emitir suas respectivas notas fiscais e faturas em observância às regras de retenção dispostas na instrução normativa RFB 1.234/2012, conforme art. 5º da portaria conjunta SEPLAN e SEFAZ nº 001, de 22 de agosto de 2022.
5.15 A **CONTRATADA** regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e

contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de Declaração, conforme IN/SRF nº 1.234/2012.
5.16 Os pagamentos efetuados à **CONTRATADA** não a isentará de suas obrigações e responsabilidades vinculadas ao fornecimento de licenciamento/execução de serviços, especialmente aquelas relacionadas com a qualidade deles.
5.17 **CONTRATADA** fica ciente da condição de que o TJMA, em atendimento às disposições do Art. 34 da Lei 10.833 de 29/12/2003 e Instrução Normativa SRF nº 1.234/2012 de 11/01/2012, poderá haver retenção na fonte, nos pagamentos efetuados, dos seguintes impostos e contribuições: Imposto de Renda Pessoa Jurídica – IRPJ; Contribuição Social sobre o Lucro Líquido – CSLL; Contribuição para o Financiamento da Seguridade Social - COFINS; e Programa de Integração Social – PIS/PASEP.

5.17.1 A retenção poderá ser efetuada aplicando-se a alíquota prevista no Anexo I da IN 1.234/2012, de 11/01/2012 e suas alterações.
5.18 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como por exemplo obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a **CONTRATADA** providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o **CONTRATANTE**;
5.19 Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos devem ser instruídos com as justificativas e motivos, e ser submetidos à apreciação da autoridade superior competente, que adotará as providências para verificar se é ou não o caso de apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a que deu causa
5.20 Nos casos de eventuais atrasos de pagamento, desde que a LICITANTE vencedora não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pelo TJMA, entre a data acima referida e a correspondente ao efetivo pagamento da nota fiscal/fatura será calculado por meio da aplicação da seguinte fórmula:

EM = I x N x VP
Em que:
EM = Encargos Moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela pertinente a ser paga;
TX = Percentual da taxa anual = 6% I = Índice de compensação financeira, assim apurado:
I = (TX/100) I = (6/100) I = 0,00016438 365 365
365 365

5.21 O TJ-MA, observados os princípios do contraditório e da ampla defesa, poderá deduzir, cautelar ou definitivamente, do montante a pagar à **CONTRATADA.**

CLÁUSULA SEXTA – DA EXECUÇÃO

6.1 Após a assinatura do Contrato pelas partes envolvidas, deverá ocorrer imediatamente a execução da renovação das licenças com upgrade e no Suporte técnico da solução Kaspersky.

6.2 O direito de uso, atualização e suporte à solução Kaspersky terá vigência contados imediatamente após a assinatura do contrato.

6.3 Constatada inconsistência entre o serviço contratado frente ao licenciamento disponibilizado, a **CONTRATADA** deverá corrigi-los, no prazo de 5 (cinco) dias úteis contados a partir da notificação efetuada pelo **CONTRATANTE**, sem qualquer ônus adicional.

6.4 Caberá à **CONTRATADA** a responsabilidade pela disponibilização das licenças, assim como a prestação dos serviços, sem qualquer ônus adicional ao TJMA;

6.5 Deverá ser entregue juntamente com os licenciamentos disponibilizados, assim como serviços prestados, as respectivas notas fiscais e/ou faturas.

6.6 Por ocasião do recebimento provisório/definitivo dos serviços, será assinado documento pertinente, em conformidade com o estabelecido no Art. 73, da Lei 8.666/1993.

6.7. Instrumentos de Solicitação de Suporte (Art. 18, § 3º, III, a, 3)

6.7.1 Abertura em central de atendimento único para todos os serviços;

6.7.2 Serão utilizados os seguintes instrumentos formais de solicitação do(s) serviço(s):

6.7.2.1 Atendimento e chamado técnico através de e-mail, site na Internet da **CONTRATADA**, e/ou canal telefônico gratuito 0800 ou custo de ligação local para São Luís-MA, 24x7 (vinte e quatro horas por dia, sete dias por semana);

6.7.3 No provimento deste serviço por meio de telefone (0800), a **CONTRATADA** fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

6.7.4 No caso de a **CONTRATADA** optar pelo atendimento por Website, deverá ser possível que o TJMA indique uma lista de produtos por meio de arquivo anexo ou diretamente na página, em um único registro. Neste caso, a data e hora do registro serão consideradas como horário da abertura do chamado para todos os produtos listados.

6.7.5 A **CONTRATADA** deverá permitir que o TJMA acompanhe o estado de chamados abertos no Centro de Assistência Técnica do fabricante por meio de site da Internet. O acesso ao Centro de Assistência Técnica deverá estar disponível durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano, passível de penalidade em caso de descumprimento, conforme descrito no item Sanções e Penalidades no Termo de Referência.

6.7.6 O horário de abertura de chamado será determinado conforme abaixo:

6.7.6.1 Para chamados abertos pelos canais 0800 ou Call Center → o horário da abertura do chamado será a data e hora da ligação realizada pelo profissional do TJMA informando do problema ocorrido. Caso a atendente não possa informar o número do chamado neste momento, o mesmo deverá, obrigatoriamente, informar um número de protocolo que registre a data e hora da ligação realizada.
6.7.6.2 Para chamados abertos pelo canal Website → o horário da abertura do chamado será a data e hora do acesso ao Website para registro do problema ocorrido. No momento do registro, a página web deverá informar o número do chamado. Caso isso não seja possível, a mesma deverá informar um número de protocolo que registre a data e hora do acesso realizado.

6.7.6.3 No caso de e-mail o horário da abertura do chamado será a data e hora de envio da mensagem pelo profissional do TJMA informando do problema ocorrido.
6.7.7 O horário de abertura do chamado marcará o início da contagem do prazo de solução das ocorrências, independente do retorno da **CONTRATADA**.
6.7.8 O horário de abertura do chamado marcará o início da contagem do prazo de retorno.
6.7.9 Não deverá haver qualquer limitação para o número de técnicos do TJMA autorizados a abrir chamados técnicos.
6.8 Local e horário de Execução do Serviço e Mecanismos Formais de Comunicação
6.8.1 A execução dos serviços presenciais deverá ocorrer no seguinte endereço, após agendamento prévio com o fiscal técnico ou seu substituto: Tribunal de Justiça do Maranhão - Praça D. Pedro II, s/n - Centro, São Luís – Maranhão.
6.8.2 A prestação dos serviços presenciais de suporte técnico deverá ocorrer, por via de regra, de segunda a sexta feira, entre 8h e 18h, salvo situações atípicas, desde que acordado previamente entre as partes;
6.8.3 Os serviços serão solicitados mediante a abertura de um “chamado”, efetuado por técnicos do **CONTRATANTE**, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português - para o horário comercial - horário oficial de Brasília).
6.9 Acompanhamento da Prestação do Suporte técnico (Art. 18, § 3º, III, a, 4)
6.9.1 Serão considerados para efeitos do suporte técnico:
6.9.1.1 **Prazo de Atendimento**: Tempo decorrido entre a abertura do chamado técnico efetuado pelo TJMA na Central de Atendimento da **CONTRATADA** e o efetivo início dos trabalhos de suporte.
6.9.1.2 **Prazo de Reparo / Solução Definitiva**: Tempo decorrido entre a abertura do chamado técnico efetuado pelo TJMA na Central de Atendimento da **CONTRATADA** e a efetiva recolocação da solução em pleno estado de funcionamento.
6.9.1.3 **Prazo de Reação**: Tempo necessário para que o TJMA receba as devidas recomendações para medidas de resposta.
6.9.2 A contagem do prazo de solução definitiva de cada chamado será a partir da

abertura do chamado técnico na Central de Atendimento disponibilizado pela **CONTRATADA**, até o momento da comunicação da solução definitiva do problema e aceite pelo Departamento de Conectividade do TJMA.
6.10 As características do suporte técnico são:
6.10.1 **Período do serviço**: 36 (trinta e seis) meses;
6.10.2 **Tempo de Resposta / Atendimento**: Varia conforme severidade;
6.10.3 **Horário Comercial de Atendimento**: 08h às 18h, de segunda a sextas-feiras;
6.10.4 **Tempo de reparo / solução**: varia de acordo com a severidade;
6.10.5 O prazo de solução poderá ser prorrogado, de acordo com as tratativas do atendimento, mediante aprovação prévia do Fiscal Técnico do Contrato;

6.10.6 Em casos comprovados em que a resolução da solução dependa exclusivamente do fabricante, o prazo poderá ser prorrogado, conforme definido entre os fiscais e a empresa **CONTRATADA**;
6.10.7 **Intervalo de cobertura**: 24 x 7 (24 horas por dia, 7 dias por semana)
6.10.8 **Suporte a distância/remoto**: Assistência remota para solução de problemas comuns de suporte.
6.10.9 Realizar eventos periódicos de manutenção remota com atualização de subsistemas, implementação de novas rotinas, implantação de novas features/funcionalidades:
6.10.9.1 Serão prestados eventos remotos de atualização periodicamente conforme definido em tabela de execução de serviços aprovada pelo fiscal técnico.
6.10.10 Todo e qualquer procedimento de atualização remota deve ser programado, previamente, entre a **CONTRATADA** e o fiscal técnico ou fiscal técnico substituto, através de e-mail.
6.11 Indicadores para os serviços de suporte técnico
6.11.1 Os serviços serão medidos, controlados e acompanhados pelo **CONTRATANTE** durante o período de vigência do contrato, com os acordos de níveis de serviço desejado e suas respectivas notificações ou penalidades.
6.11.2 Serão considerados os seguintes aspectos:
6.11.2.1 As medições dos indicadores de nível de serviço serão aferidas pelo(s) fiscal(is) técnicos da **CONTRATADA**.
6.11.2.2 O não cumprimento de um ou mais indicadores de nível de serviço ocasionará a aplicação de notificação ou penalidade à **CONTRATADA**.
6.11.2.3 O **CONTRATANTE** poderá avaliar as justificativas fundamentadas apresentadas pela **CONTRATADA** para a não aplicação das notificações ou penalidades.
6.11.3 Ao abrir um chamado relativo ao serviço de suporte técnico, o **CONTRATANTE** poderá classificá-lo em até 4 (quatro) níveis de severidade.
6.11.4 A **CONTRATADA** deverá respeitar os seguintes indicadores para o suporte técnico da solução:
Tabela de severidade - **Para problemas de funcionamento da solução *Kaspersky***

Endpoint Security

Tipo de Severidade	Tempo de Resposta	Tempo de Reparo	Descrição da Severidade
Severidade 01 – Urgente	Até 1 hora*	Até 6 horas	Problemas que tornem a infraestrutura de rede inoperante;
Severidade 02 – Alto	Até 4 horas	Até 24 horas	Problemas ou dúvidas que prejudiquem a operação da infraestrutura de rede, mas não interrompa o acesso aos dados;
Severidade 03 – Médio	Até 6 horas	Até 36 horas	Problemas ou dúvidas que criem algumas restrições a operação da infraestrutura;
Severidade 04 – Baixo	Até 8 horas	Até 48 horas	Problemas ou dúvidas que não afetem a operação da infraestrutura.

* Para garantir este tempo de resposta, o chamado deve ser aberto por telefone.

6.11.5 O nível de severidade será atribuído pelo TJMA no momento da abertura do chamado.

6.11.6 Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento.

6.11.7 A **CONTRATADA** deverá prover suporte remoto/presencial para a(s) solução(ões) ofertada(s), durante o período de vigência de suporte e manutenção, assegurando prazos de atendimento de 24 (vinte e quatro) horas por dia e sete (7) dias por semana.

6.11.8 Toda e qualquer despesa decorrente do suporte remoto ou “on site” desses atendimentos serão de responsabilidade da **CONTRATADA**.

6.11.9 No atendimento dos chamados, para efeitos de apuração do tempo gasto pela **CONTRATADA** para a Disponibilização da Solução, serão desconsiderados os períodos em que o TJMA estiver responsável por executar ações necessárias para a análise e solução da ocorrência.

6.11.10 Em quaisquer casos e quando necessário, a **CONTRATADA** deverá enviar informações, para o e-mail dos fiscais técnicos, sobre as correções a serem aplicadas ou a própria.

6.11.11 Caso não haja manifestação da **CONTRATADA** dentro do prazo definido na tabela de severidade ou caso o Fiscal do Contrato entenda ser improcedente a justificativa apresentada, será iniciado processo de sugestão de aplicação de penalidades previstas, conforme o Indicador para o suporte técnico transgredido.

6.11.12 Após a conclusão do suporte, a **CONTRATADA** comunicará o fato ao Fiscal Técnico e solicitará autorização para o fechamento do chamado. Caso o mesmo não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja

efetivamente solucionado pela **CONTRATADA**. Nesse caso o Fiscal Técnico informará as pendências relativas ao chamado aberto.
6.11.13 Sempre que houver quebra dos Indicadores para o suporte técnico o(s) fiscal(is) técnico(s) emitirá(ão) notificação a **CONTRATADA**, ou seu preposto, que terá o prazo de, no máximo, 05 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.
6.11.14 Caso não sejam observados os prazos para atendimentos previstos, ou ainda se a justificativa apresentada não for aceita pelos fiscais responsáveis do Contrato, a **CONTRATADA** estará sujeita a multas/glosas, calculadas sobre o valor descrito mensal do contrato.

6.11.15 As soluções deverão realizar upload automático de logs (diagnósticos) pelo sistema, para o fabricante, de forma a permitir diagnósticos mais eficazes.
6.11.16 Caso haja descumprimento dos indicadores por problemas alheios ao **CONTRATANTE**, e se as justificativas apresentadas pela **CONTRATADA** forem consideradas insuficientes pela fiscalização, será aplicado desconto ao valor mensal do serviço contratado conforme o disposto abaixo:

SEVERIDADE	DESCRIÇÃO	PENALIDADE
1	Prazo de Solução	Multa de 0,08% sobre o valor total do contrato, aplicada em dobro na sua reincidência. Com 1 (um) dia de atraso, multa de 0,16%.
2	Prazo de Solução	Multa de 0,05% sobre o valor total do contrato, aplicada em dobro na sua reincidência. Com 1 (um) dia de atraso, multa de 0,10%.
3	Prazo de Solução	Multa de 0,02% sobre o valor total do contrato, aplicada em dobro na sua reincidência. Com 2 (dois) dias de atraso, multa de 0,04%.
4	Prazo de Solução	Multa de 0,02% sobre o valor total do contrato, aplicada em dobro na sua reincidência. Com 3 (três) dias de atraso, multa de 0,04%.

6.11.17 A aplicação das multas acima descritas estará restrita ao máximo de 02 (duas) ocorrências (chamados técnicos), podendo ser acumulado os valores de multa quando alterado a severidade pelo fiscal técnico, durante a vigência do contrato.
6.11.18 O atraso no prazo de solução de qualquer severidade disposta na tabela de severidade superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.
6.11.19 As penalidades previstas neste instrumento não excluem aquelas dispostas na Lei nº 8.666/93.

6.12 Por ocasião do recebimento provisório/definitivo dos softwares/serviços, será assinado documento pertinente, em conformidade com o estabelecido no Art. 73, da Lei 8.666/1993.
6.12.1 Forma de Recebimento Provisório
6.12.1.1 Será considerado o recebimento provisório do objeto desta contratação mediante a efetiva entrega ao TJMA.
6.12.1.2 Quando desta entrega, será realizado o recebimento provisório, para efeito de posterior verificação da conformidade dos produtos com as especificações constantes do Termo de Referência;

6.12.1.3 O fiscal técnico após a comprovação do perfeito funcionamento do serviço/software emitirá e assinar, em no máximo 5 (cinco) dias úteis, contados do primeiro dia útil posterior à entrega dos serviços/softwares, o Termo de Recebimento Provisório.
6.12.1.4 Os serviços/softwares poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias úteis, a contar da notificação do **CONTRATANTE**, às suas custas, sem prejuízo da aplicação das penalidades.
6.12.2 Forma de recebimento definitivo
6.12.2.1 No recebimento e aceitação dos softwares/serviços, serão observadas as especificações contidas no Termo de Referência e as disposições contidas nos Artigos 73 a 76 da Lei nº 8.666/93 e Lei nº 10.520/02, e suas alterações.
6.12.2.2 As especificações serão avaliadas, também, por meio de documentos que os acompanham, informações fornecidas pela **CONTRATADA** e as disponíveis no site do fabricante.
6.12.2.3 Apresentado o Termo de Recebimento Definitivo e a Nota Fiscal Eletrônica devidamente acompanhada dos documentos solicitados no Termo de Referência ao Fiscal Técnico, este deve atestá-la, encaminhando-a, com o Termo de Recebimento Definitivo, ao Fiscal Administrativo, que após proceder a devida análise no exercício das atribuições regulamentares previstas no art. 2º, XII, alínea c, da Resolução 182/CNJ, encaminhando-a, posteriormente, ao departamento responsável ao pagamento, com as certidões cabíveis para o feito.
6.12.2.4 Se, a qualquer tempo, vier a ser constatado que o serviço/software fora fornecido em desacordo com as especificações e, em decorrência desse fato, verificar qualquer tipo de mal funcionamento da solução, o reparo desta ou, se for o caso, a sua substituição, será de inteira responsabilidade da **CONTRATADA**.
6.12.2.5 Ocorrendo qualquer problema, a **CONTRATADA** terá o prazo de 10 (dez) dias corridos para proceder às correções a partir da notificação, adequação ou substituição do objeto deste ajuste.
6.12.2.6 Caso estes não atendam ao especificado ou apresentem defeitos, serão considerados não entregues e a contagem do prazo de entrega não será interrompida

devido à rejeição deles. Neste caso, a **CONTRATADA** arcará com o (s) ônus decorrente (s) deste atraso, passível de penalidade, conforme disposto no item Sanções e Penalidades no Termo de Referência.
6.12.2.7 O aceite e o posterior pagamento dos softwares/serviços não exime a **CONTRATADA** das responsabilidades pela correção de todos os defeitos, falhas e quaisquer outras irregularidades.
6.13 Da Assistência Técnica durante o período de validade das licenças

6.13.1 A empresa fornecedora deve garantir serviços de atendimento e suporte técnico, pelo período de validade das licenças, através de telefone ou via web. Atendimento em língua portuguesa (BR).
6.13.2 A **CONTRATADA** deverá, durante a vigência do contrato, sem ônus adicional para o **CONTRATANTE**, fornecer novas versões da solução que forem lançadas para correções de falhas na aplicação (bugs) ou atualizações e melhorias das licenças adquiridas.
6.13.3 Os serviços de suporte deverão incluir os custos de pessoal, deslocamento e insumos, impostos e os demais custos que eventualmente sejam necessários, sem nenhum ônus adicional para o **CONTRATANTE**, exceto quando o defeito tiver sido consequência de negligência ou mau uso da solução.
6.13.4 Não há limitação para o número de chamados de Suporte.
6.13.5 Forma de atendimento: remoto ou presencial. No caso de atendimento remoto, a **CONTRATADA** deve informar por e-mail o fiscal técnico do contrato, assim que o atendimento for iniciado, e após a conclusão, contendo evidência das atividades executadas. Caso haja necessidade de intervenção local, esta poderá ser executada.
6.13.6 A **CONTRATADA** deve realizar semestralmente durante a vigência do contrato, um Assessment no ambiente computacional do TJMA, com o objetivo de atualizar ferramenta e time técnico de acordo com as melhores práticas.

CLÁUSULA SÉTIMA – DA DIREITO DE PROPRIEDADE INTELECTUAL
7.1 Em conformidade com o art. 111, da Lei nº 8.666, de 1993, devem ser preservados os direitos autorais e intelectuais dos produtos gerados durante a vigência do Contrato, porquanto são do **CONTRATANTE** todos os direitos de propriedade intelectual e direitos autorais associados ao material produzido em suas dependências, nas seguintes condições:
7.1.1 Nos quesitos desenvolvimento e sustentação de softwares, ambos são documentos com informações de propriedade permanente e direitos exclusivos do Poder Judiciário do Estado do Maranhão, sendo terminantemente proibida qualquer forma de compartilhamento, distribuição ou publicação.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DO CONTRATANTE

8.1 Designar formalmente, na forma do art. 67, da Lei nº 8.666/93, representantes para gerenciar e exercer a fiscalização da execução do contrato, independentemente do acompanhamento e controle exercido pela **CONTRATADA**.

8.2 Notificar a **CONTRATADA** quanto a irregularidades ou defeitos verificados na execução das atividades objeto do Termo de Referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o **CONTRATANTE**;

8.3 Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos, por intermédio de profissional especialmente designado, o qual anotará em registro próprio as falhas detectadas e as medidas corretivas necessárias. O mesmo deverá acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução fiel e correta dos serviços, podendo, ainda, sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos avençados.

8.4 Proporcionar todas as condições indispensáveis ao bom cumprimento das obrigações avençadas, inclusive permitir acesso aos profissionais ou representantes da **CONTRATADA** às suas dependências, quando necessário, e aos equipamentos e às soluções de software relacionados à execução do(s) serviço(s), mas com controle e supervisão das áreas técnicas;

8.5 Exigir o cumprimento de todos os compromissos assumidos pela **CONTRATADA**, de acordo com os termos do contrato assinado.

8.6 Proporcionar todas as condições e prestar as informações necessárias para que a **CONTRATADA** possa cumprir com suas obrigações, dentro das normas e condições contratuais.

8.7 Prestar, por meio do Fiscal Técnico do Contrato, as informações e os esclarecimentos pertinentes aos serviços avençados, que por ventura venham a ser solicitados pela **CONTRATADA**;

8.8 Informar à **CONTRATADA** sobre atos que possam interferir direta ou indiretamente nos serviços prestados;

8.9 Comunicar oficialmente à **CONTRATADA** quaisquer falhas verificadas no cumprimento do contrato, determinando, de imediato, as providências necessárias à sua regularização.

8.10 Registrar e oficializar a **CONTRATADA** sobre as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução do contrato, para as devidas providências.

8.11 Rejeitar, no todo ou em parte, os serviços que não atendam às especificações técnicas do Termo de Referência.

8.12 Aprovar ou rejeitar, no todo ou em parte, os serviços que não estiverem em conformidade com as especificações constantes da proposta apresentada pela **CONTRATADA.**

8.13 Efetuar o pagamento devido pela prestação dos serviços, desde que cumpridas todas as formalidades e exigências avençadas.
8.14 Aplicar as sanções previstas em contrato, assegurando à **CONTRATADA** o contraditório e a ampla defesa.
8.15 A forma de prestação de informações e esclarecimentos será por e-mail do fiscal técnico com cópia para o *e-mail* do fiscal substituto.
8.16 Exigir, sempre que necessário, a apresentação da documentação pela **CONTRATADA** que comprove a manutenção das condições que ensejaram a sua contratação

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATADA
9.1 Manter atualizados seus dados cadastrais junto ao Tribunal de Justiça do Estado do Maranhão.
9.2 Responsabilizar-se pelo perfeito funcionamento do objeto da contratação. Isso significa que eventual omissão técnica constante neste documento deva ser suprida pela **CONTRATADA**, sem ônus adicional a este Tribunal de Justiça.
9.3 Caberá à **CONTRATADA** a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no TJMA, quando estiver de maneira presencial realizando serviços, com todas as despesas de transporte, frete e seguro correspondentes.
9.4 Credenciar devidamente um Preposto para representá-lo em todas as questões relativas ao cumprimento dos serviços, de forma a garantir a presteza e a agilidade necessária ao processo decisório e para acompanhar a execução dos serviços e realizar a interface técnica e administrativa com o TJMA e a equipe da **CONTRATADA**, sem custo adicional.
9.5 Assumir total responsabilidade pela execução dos serviços contratados, obedecendo ao que dispõe a proposta apresentada e observando as constantes do contrato e seus anexos, inclusive reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, vícios ou incorreções que forem detectados.
9.6 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços objeto do Termo de Referência, não podendo invocar, posteriormente, desconhecimento para cobrança de serviços extras.
9.7 Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.
9.8 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem vícios, defeitos ou incorreções que forem detectados durante a vigência do instrumento contratual, cuja responsabilidade lhe seja atribuível, exclusivamente.
9.9 Garantir a prestação dos serviços, mesmo em estado de greve da categoria, através de esquema de emergência;
9.10 Arcar com qualquer custo trabalhista em virtude da jornada de trabalho dos profissionais que vier a disponibilizar para a prestação de serviços.

9.11 Manter seus empregados identificados por crachá e uniformizados, quando nas dependências do **CONTRATANTE**, devendo substituir, no prazo estabelecido por ele, qualquer um deles que for inconveniente à boa ordem, demonstre incapacidade técnica, perturbe a ação da fiscalização, não acate as suas determinações ou não observe às normas internas.

9.12 Dar ciência aos empregados do conteúdo do contrato e das orientações contidas neste documento;
9.13 Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus técnicos, na execução do serviço, ou em conexão com ele, ainda que acontecido em dependências do **CONTRATANTE.**
9.14 Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais/distrital, em consequência de fato a ela imputável e relacionado com o objeto do contrato.
9.15 Manter, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da assinatura do mesmo.
9.16 Comunicar ao **CONTRATANTE**, de imediato e por escrito, qualquer irregularidade verificada durante a execução do objeto, para a adoção das medidas necessárias à sua regularização.
9.17 Não transferir a outrem, no todo ou em parte, a execução do contrato;
9.18 Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir;
9.19 Responsabilizar-se pela conduta do empregado que for incompatível com as normas do **CONTRATANTE**, tais como: cometimento de ato desidioso, negligência, omissão, falta grave, violação do dever de fidelidade, indisciplina no descumprimento de ordens gerais e sigilo e segurança da informação;
9.20 Receber as observações do Fiscal Técnico do contrato, relativamente ao desempenho das atividades, e identificar as necessidades de melhoria;
9.21 Permitir a fiscalização e o acompanhamento da execução do objeto do Termo de Referência por servidor designado pelo **CONTRATANTE**, em conformidade com o artigo 67 da Lei nº 8.666/93;
9.22 Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias, nos termos do art. 65, § 1º da Lei 8.666/93;
9.23 Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais a que o **CONTRATANTE** for compelido a responder em decorrência desta avença.
9.24 Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços da relação contratual mantida com o **CONTRATANTE.**

9.24.1 A **CONTRATADA** deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante os procedimentos de atualização, suporte e serviços especializados, manutenção e suporte.
9.25 Responsabilizar-se técnica e administrativamente pelo objeto do contrato, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

9.26 Prestar os serviços contratados por meio de equipe técnica certificada na solução fornecida.
9.27 Não embaraçar ou frustrar a fiscalização e o acompanhamento da execução do objeto do Termo de Referência por servidor designado pelo **CONTRATANTE**.
9.28 Não subcontratar, ceder ou transferir, total ou parcialmente o objeto desta contratação.
9.29 Manter atualizada a documentação comprobatória da qualificação dos profissionais alocados na execução do serviço e disponibilizar essa documentação ao Tribunal sempre que solicitada
9.30. Os contratos e aditivos deverão ser assinados através da assinatura eletrônica, assinatura digital ou certificado digital, em conformidade com a Infraestrutura de Chaves Públicas Brasileira – ICP Brasil;

CLÁUSULA DEZ – DO REAJUSTE DE PREÇOS
10.1. Os preços permanecerão fixos e irreajustáveis, salvo quando comprovadas as situações descritas no artigo 65, inciso I, letra “b”, inciso II, letra “d” da Lei n° 8.666/93

CLÁUSULA ONZE – DAS PENALIDADES ADMINISTRATIVAS
11.1 Independente de outras sanções legais e das cabíveis penais, pela inexecução total ou parcial da contratação, a administração poderá, garantida a prévia defesa, aplicar à **CONTRATADA**, segundo a extensão da falta cometida, as seguintes penalidades, previstas no art. 87, da Lei n. 8.666/93:
11.1.1 Advertência, por escrito, nas hipóteses de execução irregular da contratação, fora dos padrões técnicos que não resulte em prejuízo para o serviço deste Tribunal de Justiça;
11.1.2 Aplicação de multa administrativa, além daquelas previstas no item 6.11.16;
11.1.2.1 Na ordem de 20% (vinte por cento) sobre o valor total da contratação, nas hipóteses de inexecução total ou violação do sigilo.
11.1.2.2 Na ordem de 0,5% do valor total da contratação, ao dia de suspensão ou interrupção, total ou parcial, salvo motivo de força maior, caso fortuito ou autorização do fiscal, dos serviços de suporte técnico e serviços profissionais, limitado ao total de 10%, moratório.

11.1.2.3 Na ordem de 1% sobre o valor da Nota Fiscal em questão, ao dia pelo não cumprimento do conteúdo disposto nos itens 6.7.5, 6.12.2.6 e 5.3.3 limitado ao total de 20%.
11.1.2.4 Caso os limites dos subitens 11.1.2.2 e 11.1.2.3 sejam excedidos, configura-se então casos de inexecução contratual.
11.1.3 Declaração de inidoneidade para licitar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida a reabilitação, na forma da lei, perante a própria autoridade que aplicou a penalidade, de acordo com o inciso IV, do art. 87, da Lei 8.666/93.
11.2 A critério da Administração, a **CONTRATADA** poderá ficar impedida de licitar e contratar com o TJMA pelo prazo de até 05 (cinco) anos, com fundamento no art. 7º, da Lei 10.520/2002, se convocado dentro do prazo de validade da sua proposta, não iniciar os serviços, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, comportar-se de modo inidôneo ou cometer fraude fiscal, sem prejuízo das multas previstas no contrato.
11.3 Considera-se também inexecução parcial do contrato, para fins de aplicação de penalidade, a não comprovação de manutenção das condições de habilitação e regularidade fiscal e trabalhista exigidas no certame;
11.4 No caso de descumprimento das demais condições previstas neste documento, no edital ou no contrato onde não haja previsão de sanções específicas, verificando-se qualquer tipo de dano ou prejuízo ao erário, poderá ser aplicada a multa de 1% por dia, incidente sobre o valor mensal da contratação até o limite de 20% (vinte por cento), ou ser caracterizado descumprimento parcial da contratação, mediante processo administrativo, garantida a ampla defesa.
11.5 O não atendimento quanto a substituição do bem/serviço defeituoso ensejará a aplicação da seguinte penalidade à **CONTRATADA**: multa diária por atraso injustificado de 5% (cinco por cento) sobre o valor unitário do item, por dia de atraso.
11.6 As sanções serão publicadas no Diário Oficial e, obrigatoriamente, registradas no SICAF e, no caso de impedimento de licitar e contratar com o PJMA, alcançando os órgãos e entidades da Administração Pública Estadual e descredenciamento, por igual período, no SICAF, sem prejuízo das multas previstas neste instrumento.
11.7 Quando do início da prestação dos serviços/entrega dos materiais, expirados os prazos propostos sem que a **CONTRATADA** o faça, iniciar-se-á a aplicação da penalidade de multa de mora, correspondente a 0,5% (meio por cento) por dia de atraso injustificado ou cuja justificativa não tenha sido acatada pela Administração deste Egrégio Tribunal de Justiça, incidente sobre o valor total do contrato.
11.8 A multa prevista no item anterior será aplicada até o limite de 20 (vinte) dias. Após o 20º (vigésimo) dia, os equipamentos / sistemas e serviços poderão, a critério da Administração, não mais ser aceitos, configurando a inexecução total da contratação, com as consequências prescritas em lei, no ato convocatório e no instrumento contratual.

11.9 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
11.10 Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo.
11.11 Se a **CONTRATADA** não recolher o valor da multa que porventura lhe for imposta, dentro de 5 dias úteis, a contar da data da notificação do responsável, o valor devido será objeto de inscrição na Dívida Ativa Estadual para posterior execução judicial e/ou será passível de protesto.
11.12 Em caso de inexecução de prestação de serviço, este TJMA garante o direito de compensação dos créditos até então auferidos pela **CONTRATADA**.
11.13 Do ato que aplicar a penalidade, caberá recurso no prazo de 5 (cinco) dias úteis, a contar da ciência da intimação, podendo a Administração reconsiderar sua decisão, dentro do mesmo prazo.

CLÁUSULA DOZE – DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

12.1 Compete à Diretoria de Informática e Automação do Tribunal de Justiça a gestão e a fiscalização deste contrato, conforme art. 3º, § 3º da Resol-GP-212018.
12.2 Os servidores responsáveis pela gestão e fiscalização estão designados na Portaria anexa a este contrato.
12.3 As atribuições do gestor e do fiscal do contrato são aquelas definidas na RESOL-GP-212018, publicada em DJE nº 54/2018 do dia 02/04/2018.
12.4 A presença de fiscalização do Tribunal de Justiça não elide, nem diminui a responsabilidade da empresa **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

CLÁUSULA TREZE - DO TRATAMENTO E DA PROTEÇÃO DE DADOS PESSOAIS

13.1. Ao participar de processo licitatório promovido por este TJMA, o licitante - titular dos dados - registra a manifestação livre, informada e inequívoca pela qual concorda com o tratamento de seus dados pessoais para finalidade específica, em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).
13.1.1. A empresa - titular dos dados – está ciente de o **CONTRATANTE** - controlador dos dados –,sempre que possível, tomar decisões referentes ao tratamento de seus dados pessoais, bem como realizar o tratamento de tais dados, envolvendo operações como as

de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
13.1.2. O **CONTRATANTE** - controlador - fica autorizado a compartilhar os dados pessoais do Titular com outros agentes de tratamento de dados, caso seja necessário para finalidade específica, observados os princípios e as garantias estabelecidas pela Lei nº 13.709, de 14 de agosto de 2018.

13.2. Caberá à **CONTRATADA** e ao **CONTRATANTE** proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, garantindo que:
13.2.1. O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos Arts. 7º e/ou 11 da Lei nº 13.709/2018 o qual se submete o objeto deste Edital, e para propósitos legítimos, específicos, explícitos e informados ao titular, respeitadas as regras previstas pelos artigos 23 a 30 da Lei nº 13.709/2018.
13.2.2. O tratamento seja limitado às atividades necessárias para atingir as finalidades de execução do objeto contratado.
13.2.3. Os sistemas, que servirão de base para armazenamento dos dados pessoais coletados, deverão seguir as políticas de segurança e acesso determinado pela Política de Proteção de Dados Pessoais e da Privacidade do **TJMA**.
13.2.4 Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a **CONTRATADA** interromperá o tratamento dos dados pessoais disponibilizados pelo **CONTRATANTE** e eliminará completamente os dados pessoais e todas as cópias porventura existentes, seja em formato digital ou físico, salvo quando a **CONTRATADA** tenha que manter os dados para cumprimento de obrigação legal ou outra hipótese da LGPD.
13.3. O **CONTRATANTE** poderá manter e tratar os dados pessoais do Titular durante todo o período em que eles forem pertinentes ao alcance das finalidades listadas neste edital.
13.3.1. Dados pessoais anonimizados, sem possibilidade de associação ao indivíduo, poderão ser mantidos por período indefinido.
13.3.2. O Titular poderá solicitar ao **CONTRATANTE**, a qualquer momento, que sejam eliminados os seus dados pessoais não anonimizados, desde que não autorizada a conservação para finalidades previstas em lei.
13.4. O Titular tem direito a obter do **CONTRATANTE** a relação dos dados por ele tratados, a qualquer momento e mediante requisição, conforme art. 18, capítulo III, LGPD.
13.5. O **CONTRATANTE** responsabiliza-se pela manutenção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

13.5.1. Em conformidade ao art. 48 da Lei nº 13.709/2018, o Controlador comunicará ao Titular e à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao Titular.

CLÁUSULA QUATORZE - DAS ALTERAÇÕES CONTRATUAIS

14.1 Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

14.2. A **CONTRATADA** é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. As supressões resultantes de acordo celebrado entre as partes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA QUINZE – DA RESCISÃO CONTRATUAL

15.1. O presente instrumento poderá ser rescindido:

a) Por ato unilateral e escrito da Administração, nos casos enumerados nos incisos I a XII, XVII e XVIII do art. 78 da Lei n° 8666/93;

b) Amigavelmente, por acordo entre as partes, reduzido a termo no respectivo procedimento administrativo, desde que haja conveniência para a Administração; ou

c) Judicialmente, nos termos da Lei.

Parágrafo Único – No caso de rescisão amigável, a parte que pretender rescindir o Contrato comunicará sua intenção à outra, por escrito.

15.2. Os casos de rescisão contratual serão formalmente motivados nos autos do Processo, assegurado o contraditório e a ampla defesa.

15.3. A rescisão por descumprimento das cláusulas contratuais acarretará a retenção dos créditos decorrentes do Contrato, até o limite dos prejuízos causados ao **CONTRATANTE**, além das sanções previstas neste instrumento.

CLÁUSULA DEZESSEIS - DA ALTERAÇÃO SUBJETIVA

16.1 É admissível a fusão, cisão ou incorporação da **CONTRATADA** com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

CLÁUSULA DEZESSETE – DA VEDAÇÃO À SUBCONTRATAÇÃO.

17.1. Não será permitida a subcontratação. O suporte técnico deverá ser prestado por profissionais da própria **CONTRATADA** da solução, com atendimento aos requisitos constantes neste instrumento.

CLÁUSULA DEZOITO – DA VINCULAÇÃO AO EDITAL DA LICITAÇÃO

18.1. O presente contrato tem fundamento a Lei 10.520/02 e subsidiariamente a Lei n.º 8.666/93, bem como suas alterações.

18.2. O **CONTRATANTE** e a **CONTRATADA** vinculam-se plenamente ao presente contrato e aos documentos que integram o Processo Administrativo n.° 26.856/2022– TJ/MA, e que são partes integrantes deste contrato, independente de transcrição, o Edital PE 08/2023, o Termo de Referência, a Proposta de Preços da **CONTRATADA**.

CLÁUSULA DEZENOVE – DA PUBLICAÇÃO

19.1 O **CONTRATANTE** providenciará a publicação de forma resumida deste Contrato, na Imprensa Oficial, em obediência ao disposto no § único do artigo 61 da Lei nº 8.666/93.

19.2 Este contrato após assinado e publicado estará disponível no Portal da Transparência do TJMA: http://www.tjma.jus.br/financas/index.php?acao_portal=menu_contratos

CLÁUSULA VINTE – DO FORO

20.1 Elegem as partes **CONTRATANTES** o Foro desta cidade, para dirimir todas e quaisquer controvérsias oriundas deste Contrato, renunciando expressamente a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e contratadas as partes, por seus representantes legais, assinam o presente Contrato de inteiro teor.

PAULO SERGIO VELTEN PEREIRA:25754548320

Assinado de forma digital por PAULO SERGIO VELTEN PEREIRA:25754548320
Dados: 2023.04.18 11:44:21 -03'00'

Desembargador PAULO SÉRGIO VELTEN PEREIRA
Presidente do Tribunal de justiça do Estado do Maranhão
[ASSINADO ELETRONICAMENTE)

YURE LEOPOLDO SABINO DE FREITAS
Representante Legal da Empresa
[ASSINADO ELETRONICAMENTE)

CTPS 0034_2023_PROC. 26856_2022_NETWORK SECURE (1).pdf

Documento número #ed6e7380-5f6a-4a1f-847f-d95e60a274be

Hash do documento original (SHA256): 288e4fc6573e77435e7912b23e091a6a0aae3c25871f76a665aeb065ec7f2fb4

Hash do PAdES (SHA256): 29d3c8c43cc0a9e6dfd565832df47ea8733cadffb69eb8ed0636afa26d184fce

Assinaturas

1 assinatura digital e 1 assinatura eletrônica

Yure leopoldo sabino de freitas

CPF: 525.285.023-20

Assinou em 11 abr 2023 às 09:24:14

Emitido por AC SOLUTI Multipla v5- com Certificado Digital ICP-Brasil válido até 30 mai 2023

THIAGO GOMES TELES

CPF: 607.722.003-51

Assinou como testemunha em 11 abr 2023 às 08:16:37

Log

11 abr 2023, 08:15:20	Operador com email thiago.teles@networksecure.com.br na Conta 3f65b887-ad53-46cb-b0d6-e806684df2bc criou este documento número ed6e7380-5f6a-4a1f-847f-d95e60a274be. Data limite para assinatura do documento: 11 de maio de 2023 (08:13). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
11 abr 2023, 08:15:47	Operador com email thiago.teles@networksecure.com.br na Conta 3f65b887-ad53-46cb-b0d6-e806684df2bc adicionou à Lista de Assinatura: yure.sabino@networksecure.com.br para assinar, via E-mail, com os pontos de autenticação: Certificado Digital; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Yure leopoldo sabino de freitas e CPF 525.285.023-20.
11 abr 2023, 08:15:47	Operador com email thiago.teles@networksecure.com.br na Conta 3f65b887-ad53-46cb-b0d6-e806684df2bc adicionou à Lista de Assinatura: thiago.teles@networksecure.com.br para assinar como testemunha, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo THIAGO GOMES TELES.
11 abr 2023, 08:16:37	THIAGO GOMES TELES assinou como testemunha. Pontos de autenticação: Token via E-mail thiago.teles@networksecure.com.br. CPF informado: 607.722.003-51. IP: 200.225.204.137. Localização compartilhada pelo dispositivo eletrônico: latitude -3.7515005 e longitude -38.5005521. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.479.0 disponibilizado em https://app.clicksign.com.

11 abr 2023, 09:24:15	Yure leopoldo sabino de freitas assinou. Pontos de autenticação: certificado digital, tipo A1 e-cpf. CPF informado: 525.285.023-20. IP: 200.225.204.137. Localização compartilhada pelo dispositivo eletrônico: latitude -3.7513656 e longitude -38.50044. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.479.0 disponibilizado em https://app.clicksign.com.
11 abr 2023, 09:24:15	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número ed6e7380-5f6a-4a1f-847f-d95e60a274be.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://validador.clicksign.com e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº ed6e7380-5f6a-4a1f-847f-d95e60a274be, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.