**PROJETO BÁSICO**

# CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DE ENPOINTS

# PROJETO BÁSICO

## 1. OBJETO E UNIDADE REQUISITANTE

1.1. Solução de Segurança de *Endpoints* com adequação da quantidade de licenças ao ambiente computacional da Justiça do Trabalho.

1.2. Unidade Requisitante: Comissão de Informática do TRT da 19ª Região.

## 2. MOTIVAÇÃO DA CONTRATAÇÃO

2.1. A utilização de sistemas de antivírus possibilita a redução dos riscos de fraude, vazamento de informações, inconsistência de informações, indisponibilidade das aplicações corporativas e, até mesmo, sabotagens que podem gerar falso repúdio.

2.2. A solução tem por objetivo prover meios para proteger endpoints (estações de trabalho e servidores de aplicações) de artefatos maliciosos, que podem causar diversos impactos negativos ao desempenho das atividades, como indisponibilidade de serviços e sistemas, vazamento de informações, invasão de ambiente tecnológico, dentre outros.

2.3. No TRT, onde a tramitação judicial dá-se por meio 100% digital, o que torna indispensável que os equipamentos possuam soluções de proteção que auxiliem na garantia da confidencialidade, integridade e confidencialidade necessárias ao bom funcionamento do ambiente tecnológico.

2.4. O contrato da atual solução vencerá em **16/06/2021**, não sendo possível a sua prorrogação devido à classificação do objeto no processo licitatório do TRT da 13ª Região que deu origem à contratação. Após essa data a solução deixará de receber as atualizações, imprescindíveis ao funcionamento desse tipo de software, além de deixar a equipe do TRT sem possibilidade de acionar o suporte técnico da solução.

2.5. A solução de proteção de endpoints é uma das iniciativas nacionais da Justiça do Trabalho, patrocinadas e custeadas pelo CSJT. Uma nova contratação para substituir a solução atual está sendo realizada por meio do Pregão Eletrônico 03/2021 do TRT da 13ª Região, no qual serão registradas licenças de uma nova solução para todos os Tribunais da JT,com a participação deste Tribunal.

2.6. Considerando que o citado Pregão Eletrônico TRT13 03/2021, que teve sua abertura marcada para o dia 16/4/2021, foi revogado e terá que ser republicado com ajustes, bem como todos os trâmites e intercorrências possíveis no processo até a contratação e instalação da nova solução neste Tribunal, caracteriza-se a necessidade de contratação emergencial para estender a validade das licenças da atual solução de proteção de endpoint, Mcafee Endpoint Security, por um período de 6 meses, considerado suficiente para que a solução a ser licitada pelo TRT13 seja implantada neste Tribunal.

2.7. Por fim, cabe justificar que esta área técnica não deu início ao processo de contratação com maior antecedência devido a se tratar de uma contratação nacional, cuja expectativa vinha sendo informada pelo órgão registrador como viável para a continuidade dos serviços, o que acabou não se concretizando.

**2.8.** **Objetivos a serem alcançados** - O principal objetivo desta demanda é garantir a proteção contra programas e softwares maliciosos para todas as estações de trabalho e servidores da Justiça do Trabalho, contribuindo para a segurança da informação e a operação dos sistemas de TIC, inclusive o Processo Judicial Eletrônico da Justiça do Trabalho.

**2.9.** **Benefícios diretos e indiretos:**

2.6.1 Redução dos riscos de segurança associados à Tecnologia da Informação.

2.6.2 Redução da quantidade de incidentes de segurança relacionados a ameaças oriundas de malwares.

2.6.3 Otimização do uso dos recursos de Tecnologia da Informação.

2.6.4 Proteção das estações e servidores contra ameaças eletrônicas tais como vírus, worms, trojans, spywares, ransonwares, entre outras.

2.6.5 Suporte técnico especializado prestado pelo fabricante do produto.

2.6.6 Solução de segurança de *endpoints* atualizada e em conformidade com as melhores práticas previstas pelo fabricante.

2.6.7 Integração com a ferramenta de proxy atualmente em uso na Justiça do Trabalho (McAfee Web Gateway).

2.6.8 Ganho de produtividade com a não parada de equipamentos por problemas com infecção de códigos maliciosos.

2.6.9 Redução de risco relacionado a vazamento de informações.

2.6.10 Melhoria de controle com maior segurança dos dados e disponibilidade dos serviços.

## 3. DISCRIMINAÇÃO E QUANTITATIVOS

3.1. A infraestrutura de TIC do TRT da 19ª Região é composta por 1250 estações e servidores físicos, bem como por 80 servidores virtuais que necessitam ser protegidos por softwares antivírus, razão pela qual torna-se obrigatória a contratação de suporte / subscrição nos quantitativos definidos na tabela abaixo:

| Item | Descrição | Demanda PJe/JT | Qtd. Total |
|---|---|---|---|
| 1 | Solução de segurança de endpoints para estações e servidores físicos com licenciamento, instalação, capacitação e suporte: multiplataforma com ePO, TIE, Controle de dispositivos, firewall integrado, HIPS, antimalware, proteção de email, controle de web com filtragem de URL e pesquisa segura | 1.250 | 1.250 |
| 2 | Solução de segurança de endpoints para servidores virtuais com licenciamento, instalação, capacitação e suporte: com ePO, TIE, GTI *file reputation* e HIPS | 80 | 80 |

# PROJETO BÁSICO

## 4. ESTRATÉGIA DE CONTRATAÇÃO

**4.1. Natureza do objeto –**

4.1.1 O objeto possui características comuns e usuais encontradas no mercado de TIC, cujos padrões de desempenho e qualidade podem ser objetivamente definidos.

4.2.2 **A contratação será realizada de forma direta em caráter emergencial, nos termos do inciso IV, artigo 24 da Lei Nº 8666/1993.**

**4.2. Parcelamento do objeto**

4.2.1 Como é necessária a compatibilidade entre os dois itens que serão licitados, e por se tratar de um único fabricante para os dois itens, não deve haver parcelamento do objeto. Ademais, concentrar os esforços de repassar informações sobre as peculiaridades dos ambientes dos TRTs para um único fornecedor, que prestará o serviço no âmbito nacional, colaborará com o processo de habilitação dos profissionais por ele contratados e, espera-se, imprimirá celeridade aos atendimentos.

4.2.2 Todo o fornecimento deve ser executado por uma única empresa, uma vez que todos os itens são da mesma natureza e do mesmo fabricante, constituindo uma solução única e integrada. A licitação em lote único não representa qualquer restrição ou prejuízo a ampla concorrência, uma vez que um canal de venda que comercialize produtos da Intel/McAfee poderá cotar todos os itens. O agrupamento em lote único também irá favorecer a obtenção de melhores preços em função da potencial economia de escala. Também pelos motivos expostos, concluímos pela inviabilidade de dividir o objeto de forma a estabelecer a cota de 25% para ME/EPP.

**4.3. Forma e critério de seleção do fornecedor**

4.3.1 Será utilizada a modalidade contratação direta em virtude da emergencialidade da situação.

4.3.2 **Classificação e Indicação Orçamentária**

4.5.1 As despesas decorrentes do objeto desta contratação serão programadas conforme descentralização orçamentária do Conselho Superior da Justiça do Trabalho.

**4.4. Vigência da Prestação de Serviço**

4.6.1 Vigência: A vigência da contratação terá início após o recebimento definitivo por parte do CONTRATANTE dos itens licitados no lote único e se estenderá por um **prazo de 6 (seis)** meses após esta data.

4.6.2 Prazo para entrega e instalação: até 5 (cinco) dias úteis, contados a partir da data de emissão do empenho.

4.6.3 Local e forma de entrega: Por meio eletrônico para setic.infra@trt19.jus.br.

4.6.4 Os recebimentos provisório e definitivo serão emitidos da seguinte forma:

- Recebimento Provisório – imediatamente após a entrega e instalação dos bens;
- Recebimento Definitivo – após realização de testes pelo CONTRATANTE em conjunto com a CONTRATADA no prazo máximo de 15 (quinze) dias corridos, pela equipe de gestão da contratação, depois de verificadas a qualidade e a quantidade do material.

4.6.5 O pagamento será mensal e a primeira parcela será paga após 30 (trinta) dias do recebimento definitivo.

### 4.5. Informações acerca do impacto ambiental

4.7.1 Os impactos ambientais são mínimos por se tratar de licenças de software e suporte técnico. De toda forma, a CONTRATADA deverá promover a correta destinação dos resíduos resultantes da prestação do serviço, tais como embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental como a Política Nacional de Resíduos Sólidos (Lei n.º 12.305/2010) e o Guia de Contratações Sustentáveis da Justiça do Trabalho (Resolução n.º 103/2012 do Conselho Superior da Justiça do Trabalho).

### 4.6. Conformidade técnica e legal

4.8.1 Segurança estabelecidas pelo Contratante para execução do objeto, tanto nas dependências do Contratante como externamente.

4.8.2 Manter sob sigilo, sob pena de responsabilidade civil, penal e administrativa, todo e qualquer assunto de interesse do Tribunal ou de terceiros de que tomar conhecimento em razão da prestação do serviço.

4.8.3 A presente contratação deve observar a Lei n.° 8.666, de 21 de junho de 1993, que institui normas para licitações e contratos da Administração Pública.

4.8.4 A presente contratação deve observar a Resolução n.º 182, de 17 de outubro de 2013, que "Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ)."

4.8.5 As especificações técnicas devem contemplar os critérios de sustentabilidade conforme preceitua a Res. CSJT n.º 103/2012.

## 5. DAS OBRIGAÇÕES CONTRATUAIS

### 5.1 Deveres e Responsabilidades da Contratante

5.1.1 Proporcionar todas as condições para que a CONTRATADA possa desempenhar seus serviços de acordo com as determinações nesse Projeto Básico.

5.1.2 Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas editalícias, contratuais e os termos de sua proposta.

5.1.3 Exercer o acompanhamento e a fiscalização dos chamados de atendimento, por servidor especialmente designado.

5.1.4 Notificar a CONTRATADA por escrito acerca da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção, caso não previsto neste instrumento.

5.1.5 Zelar para que, durante toda a vigência da contratação, sejam mantidas, em compatibilidade com as obrigações assumidas pela CONTRATADA, todas as condições de habilitação e qualificação exigidas na licitação.

5.1.6 Fornecer atestados de capacidade técnica, quando solicitado pela CONTRATADA, desde que atendidas as obrigações contratuais.

5.1.7 Receber o produto que atenda as especificações exigidas e o preço ofertado e efetuar o pagamento dentro do prazo pactuado.

5.2 **Deveres e Responsabilidades da Contratada**

5.2.1 Entregar as licenças e os serviços contratados, no prazo previsto. Caso o atendimento não seja feito dentro do prazo, a CONTRATADA ficará sujeita às sanções previstas neste Projeto Básico e Edital respectivo.

5.2.2 Apresentar documentação comprobatória da origem dos bens importados oferecidos, se for o caso, e da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa de 10% do valor do empenho.

5.2.3 Cumprir o Acordo de Nível de Serviço (SLA) estabelecido neste Projeto Básico.

5.2.4 Implantar e configurar todos os módulos da solução obedecendo aos requisitos da política de segurança da informação da CONTRATANTE.

5.2.5 Fornecer, sem qualquer ônus adicional ao CONTRATANTE, quaisquer componentes adicionais de software necessários ao perfeito funcionamento dos itens ofertados, mesmo que não constem do Projeto Básico.

5.2.6 Submeter à aprovação deste Tribunal toda e qualquer alteração ocorrida nas especificações, em face de imposições técnicas, de cunho administrativo ou legal.

5.2.7 Responsabilizar-se por todos os encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, tributos de qualquer espécie que venham a ser devidos em decorrência da execução deste instrumento, bem como custos relativos ao deslocamento e estada de seus profissionais, caso existam.

5.2.8 Responsabilizar-se pelos danos causados diretamente ao CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo, ação ou omissão, quando da execução do objeto da contratação, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento realizado pelo CONTRATANTE.

5.2.9 Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionado com esta contratação.

5.2.10 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 contratação.

5.2.11 Manter seus funcionários, quando nas dependências do CONTRATANTE, sujeitos às normas internas deste (segurança e disciplina), todos utilizando uniforme e crachá de identificação, porém sem qualquer vínculo empregatício com o Órgão.

5.2.12 Possibilitar a fiscalização deste Tribunal, no tocante à verificação das especificações exigidas neste Projeto Básico, prestando todos os esclarecimentos solicitados e atendendo às reclamações procedentes, caso ocorram.

5.2.13 Comunicar ao CONTRATANTE, de imediato e por escrito, qualquer irregularidade verificada durante a execução do objeto contratado, para a adoção das medidas necessárias à sua regularização.

5.2.14 Manter, durante toda a vigência da contratação, as condições de habilitação consignadas neste documento.

5.2.15 Para fins de comunicação entre as partes contratantes, eventuais mudanças de endereço e correio eletrônico da Contratada deverão ser comunicadas de imediato ao Contratante.

5.2.16 Indicar um preposto responsável por acompanhar a execução do objeto contratado e atuar como interlocutor principal junto ao órgão contratante.

## 6. ESPECIFICAÇÃO TÉCNICA

**6.1. ITEM 1 – Solução de segurança de endpoints para estações e servidores físicos com licenciamento, instalação, capacitação e suporte: McAfee Endpoint Protection Suite multiplataforma com ePO, TIE, Controle de dispositivos, firewall integrado, HIPS, antimalware, proteção de email, controle de web com filtragem de URL e pesquisa segura.**

a) A proteção para estação de trabalho deve contemplar, no mínimo, os seguintes módulos:

1. Módulo Anti-Malware
2. Módulo de Prevenção de Intrusos e Firewall
3. Módulo de Controle Web
4. Módulo de Proteção de E-mail
5. Módulo de Controle de Dispositivos
6. Módulo de Gerência

b) A solução deve ser gerida por uma única console;

c) Deve integrar de maneira nativa com a solução de base de dados local de ameaças.

**1. Módulo Anti-Malware – Sistemas Windows e Linux**

a) Deve prover proteção em tempo real (real-time scanning) para garantir a segurança do sistema instalado;

b) Deve possuir suporte as seguintes plataformas:

I. Windows Vista
II. Windows XP SP3
III. Windows 7 (Home/Premium/Professional/Ultimate/Enterprise)
IV. Windows 8 (Basic/Pro/Enterprise)
V. Windows 8 Patch 1
VI. Windows 10
VII. Linux Red Hat 5, 6 e 7
VIII. Linux CentOs 5, 6 e 7
IX. Protocolo 12.882/2016 8
X. Oracle Linux 5, 6 e 7
XI. Google Chrome 31 ou superior (navegador)
XII. Mozilla Firefox 34 ou superior (navegador)

c) Deve fornecer suporte total a plataforma 64 bits nas plataformas mencionadas;

d) Todas as funcionalidades deste item devem ser ativadas por agente único que facilita a instalação, a configuração e o gerenciamento.

e) Deve ser capaz de prevenir alterações não autorizadas ao sistema operacional, restringindo acesso a arquivos, compartilhamentos e chaves de registro.

f) Deve possuir o recurso de blindagem, impedindo o comprometimento dos aplicativos e dos seus dados, além de evitar que um aplicativo seja usado para atacar outros aplicativos.

g) O módulo deverá ter capacidade de proteger contra, no mínimo, modificação dos arquivos do próprio módulo de anti-malware, arquivos e configuração do Mozilla, Internet Explorer e Google Chrome e instalação de objetos do tipo "browser helper" e executar programas a partir da pasta temporária do sistema (temp);

h) Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex e outros scripts;

i) A proteção para pastas e arquivos deverá compreender a alteração, acesso (abertura) ou a deleção de arquivos e/ou pastas e chaves de registro.

j) Deve permitir ajustar a sensibilidade do nível de proteção desejado.

k) . Deve permitir que o administrador configure exceção a regra de scan, ou seja, uma pasta, arquivo ou drive que não deve ser verificado pelo processo de análise do módulo.

l) A regra de exceção de scan deve suportar o uso de wildcards (?, *).

m) Rastreamento em tempo real, para arquivos durante entrada e saída (gravação e leitura), com as seguintes opções:

I. Limpar arquivos automaticamente;
II. Excluir arquivos Automaticamente;
III. Negar Acesso aos Arquivos (quarentena);

n) Deve ter a opção de rastreamento manual com interface Windows, customizável, com opção de limpeza;

o) Permitir diferentes configurações de varredura em tempo real baseando-se em processos de baixo ou alto risco, tornando assim o desempenho do produto mais estável;

p) Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo;

q) Detecção de programas maliciosos como spyware, programas de propaganda, ferramentas como password crackers, dentre outros;

r) Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site da Internet, com frequência (no mínimo diária) e horários definidos pelo administrador;

s) Permitir atualização incremental da lista de definições de vírus;

t) Salvar automaticamente as listas de definições de vírus em local especificado na rede, após cada atualização bem-sucedida;

u) O scanner de arquivos deverá atuar integrada a camada mais baixa do sistema operacional, atuando como um interceptador de chamadas junto ao driver deste. Qualquer arquivo que seja aberto, fechado e renomeado deve ser verificado pelo módulo anti-malware.

v) Para otimizar as verificações o módulo deve possuir um cache dos arquivos verificados;

w) O cache mantido pelo módulo anti-malware deve ser atualizado (recriado) sob duas condições:

I. Atualização de Vacinas;
II. ii. Ocupação total do cache;

x) Deve ser possível habilitar ou desabilitar a verificação de arquivos em mapeamentos de rede;

y) Deve possuir um módulo de análise de scripts, atuando como um proxy entre o módulo e o componente “Windows Scripting Host” do Sistema Operacional;

z) Caso o script seja malicioso este não deverá permitir a execução do mesmo;

aa) Deve ser capaz de analisar arquivos por método heurístico;

bb) Deve permitir ao administrador configurar a sensibilidade da heurística;

cc) Deve ser possível configurar políticas diferenciadas para processos de baixo risco e de alto risco;

dd) Deve ser possível configurar e iniciar scans sob demanda;

ee) O administrador deve ter a possibilidade de ajustar a prioridade do processo de scan em contrapartida à prioridade no sistema operacional;

ff) Deve suportar os clientes de e-mail Microsoft Outlook e Lotus Notes;

gg) Deve analisar e-mails e anexos quanto a artefatos maliciosos, sendo que a análise deve ser feita quando o e-mail for recebido ou quando for acessado;

hh) Deve ser possível configurar a deleção do anexo ou do e-mail infectado;

ii) Em caso de impossibilidade na deleção, deve ser possível mover o anexo para uma pasta designada pelo administrador;

jj) Programação de rastreamentos automáticos do sistema com as seguintes opções:

I. **Escopo**: Todos os drives locais, drives específicos, ou pastas específicas;
II. **Ação**: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
III. **Frequência**: Horária, diária, semanal, mensal;
IV. **Exclusões**: Pastas ou arquivos que não devem ser rastreados;

kk) Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;

ll) Os logs deverão ser segmentados por funcionalidade, ou seja, ter um arquivo de log diferenciado por:

I. Log de Proteção de Acesso
II. Log de Proteção Contra Estouro de Buffer
III. Log de Atualização
IV. Log de Verificação sob Demanda

mm) O Log de proteção de acesso deve gravar, no mínimo, as seguintes informações em log:

I. Data
II. Hora
III. Ação Tomada
IV. Credenciais do usuário
V. Processo
VI. Localização do Processo
VII. Regra Acionada

nn) Deve ser possível registrar o evento em arquivo e posteriormente encaminhar o alerta via SNMP;

oo) Permitir bloqueio de aplicações pelo nome do arquivo;

pp) Permitir o bloqueio do compartilhamento caso uma ameaça seja detectada em uma pasta compartilhada;

qq) Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia;

rr) Deve ser capaz de bloquear comunicações de um computador que tenha comportamento malicioso (exemplo: Grava arquivos maliciosos ou programas indesejados – Cavalo de Troia) de maneira automática;

ss) Possuir proteção contra estouro de buffer;

tt) Deve ser possível enviar arquivos suspeitos para análise do Laboratório do Fabricante;

uu) Detecção de cookies potencialmente indesejáveis no sistema;

vv) O sistema de antispyware deve estar totalmente integrado ao software antivírus utilizando a mesma biblioteca DAT de definições de vírus e demais ameaças;

ww) Possuir proteção completa, pronta para operação e contra vulnerabilidades desconhecidas, tais como estouro de buffer (buffer overflow) e ataques de dia zero (zero-day attacks);

xx) A proteção contra estouro de buffer deve proteger contra:

I. Heap Attacks
II. Stack Attacks

yy) Deve ser capaz de proteger, no minimo, 30 (trinta) aplicações contra estouro de buffer, como por exemplo Internet Explorer, Microsoft Word, Microsoft Outlook e Outlook Express.

zz) Deve ser capaz de executar aplicações enjauladas, ou seja, com limitações de ações caso o aplicativo seja malicioso;

aaa) Deve ser capaz de bloquear ou alertar caso encontre algum aplicativo malicioso.

bbb) Deve ser capaz de bloquear, no mínimo, as seguintes ações para aplicativos enjaulados:

I. Acessar cookies do usuário
II. Criar novas threads em outro processo
III. Alocar memória em outro processo
IV. Criar arquivos em um destino de rede
V. Criar arquivos com extensão .bat
VI. Criar arquivos com extensão .exe
VII. Criar arquivos com extensão .htm, jpg e .bmp
VIII. Alterar as associações de arquivos;
IX. Executar algum processo "child"
X. Desabilitar executáveis chave do sistema operacional;
XI. Criar arquivos com a extensão .vbs

ccc) Caso detecte uma aplicação enjaulada maliciosa com características de Ransonware, o mesmo deve ter capacidade detecção e bloqueio especificas.

**2. Módulo de Prevenção de Intrusos e Firewall**

a) Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura contra ataques dia zero;

b) Deve ser capaz de identificar e bloquear ataques conhecidos através de assinaturas;

I. A atualização de assinaturas não deve exigir reinício do sistema operacional;

c) Deve possuir um firewall de estação statefull bloqueando tráfego de entrada e controlando o tráfego de saída;

d) Deve permitir políticas diferenciadas de acordo com o meio de conexão, como por exemplo: Rede do Orgão, ou VPN ou Rede Pública;

e) Deve proteger a estação em todos os níveis:

I. Rede;
II. Aplicação;
III. Execução no Sistema Operacional;

f) Deve fornecer proteção de Firewall até a camada 7 de rede;

g) Deve fornecer proteção contra vulnerabilidades existentes nas estações de trabalho;

h) Deve proteger contra ataques locais iniciados por CD's ou dispositivos USB;

i) Deve proteger contra ataques que trafegam por fluxos criptografados;

j) Deve proteger contra ataque de negação de serviço;

k) Deve proteger contra tentativas de invasão;

l) Deve possuir proteção contra BOTs ;

m) O módulo deve conter um conjunto de políticas pré-configuradas;

n) Deve permitir a customização de regras para melhor proteger o ambiente de estações de trabalho;

o) Deve possibilitar a configuração de regras de exceção;

p) Deve permitir a proteção contra IP spoofing;

q) Deve possuir integração com o Centro de Inteligência do fabricante para verificar a reputação do endereço IP;

r) A reputação deve informar quatro níveis:

I. Mínimo
II. Não verificado
III. Médio
IV. Alto

s) Para evitar consumo de banda, a solução deve manter um cache para este tipo de consulta;

t) Deve permitir criar regras com base nos seguintes parâmetros:

I. Descrição;
II. Ação
III. Direção
IV. Protocolo de Rede
V. Aplicação e Executáveis
VI. Tempo de aplicação da regra;

u) Deve ser possível definir uma lista de:

I. Redes Confiáveis
II. Aplicações Confiáveis;

v) Para usuários avançados, deve ser possível liberar a console de HIPS e Firewall local para a criação de regras;

w) Deve ser possível configurar uma regra de isolamento para uma determinada conexão (Cabeada ou Wireless);

x) Permitir o bloqueio de ataques baseados em Web como: Directory Traversal Attacks e Unicode Attacks;

y) Prevenir o roubo de informações de um servidor Web, ou mesmo que um hacker com privilégios de root possa manipular o servidor Web;

z) Permitir criação de política que somente permita tráfego de rede de saída da máquina depois que o cliente de IPS de Host estiver sendo executado;

aa) Bloquear acessos indevidos que não estejam na tabela de políticas definidas pelo administrador;

bb) Ao detectar uma ameaça o módulo deve ser capaz de informar o administrador através dos seguintes meios:

I. Executar uma tarefa agendada;
II. Executar comandos externos;
III. Enviar trap SNMP
IV. Enviar um Email;

cc) Interceptar tráfego e requisições de HTTP após decriptação e decodificação;

dd) Permitir criar regras de bloqueio/permissão utilizando protocolos ou aplicações;

ee) Permitir configuração de regras por horários.

ff) Oferecer proteção avançada de sistemas contra ameaças tais como ataques remotos de injeção de SQL ou HTTP;

**3. Módulo de Controle Web**

a) Possibilidade de bloqueio de sites baseados em fatores de ameaça ou avaliação do site;

b) As avaliações devem ser baseadas em:

I. Janelas de popups excessivas;
II. Tentativas de explorar vulnerabilidades no Browser
III. Práticas fraudulentas empregadas pelo site;
IV. Download de programas não desejados;
V. Analise através do Time de Inteligência do Fabricante;

c) Deve integrar com motores de busca e apresentar cores indicativas para ilustrar ao usuário o risco ou não existência de risco no site, com no mínimo:

I. Verde: Site Seguro
II. Vermelho: Algum problema grave com o Site
III. Amarelo: Algum problema com o Site
IV. Preto: Site com phishing
V. Cinza: Sem classificação

d) Deve funcionar independente de conectividade com o Módulo de Gerência;

e) Deve-se integrar com, no mínimo os seguintes motores de busca:

I. Google
II. Yahoo!
III. Ask.com
IV. Terra
V. Uol
VI. Baidu
VII. Bing
VIII. AOL

f) Deve possuir integração com, no mínimo, os seguintes browsers:

I. Internet Explorer 6 ou superior

## PROJETO BÁSICO

II. Google Chrome 13 ou superior
III. Mozilla Firefox 1.5 ou superior

g) Deve permitir o bloqueio de acesso a sites com conteúdo duvidoso ou malicioso;

h) Possibilidade de criar blacklists e whitelists de urls para estações pela console de gerenciamento;

i) Possuir módulo de proteção de navegação a determinado conteúdo na internet possuindo pelo menos 80 categorias de websites.

j) Esta categorização deve ser atualizada constantemente e automaticamente pelo fabricante a fim de prover maior qualidade deste serviço;

k) Deve ser capaz de restringir downloads com origem em sites não confiáveis ou com classificação maliciosa;

l) Ao receber um e-mail o usuário deve ser informado da classificação da URL inserida no corpo do e-mail;

m) A anotação no email deve servir para:

I. Cliente Microsoft Outlook;
II. Cliente Webmail (Gmail, Outlook.com, Aol e Yahoo)

n) Possuir pelo menos as categorias abaixo:

I. Sites de armas;
II. Sites de material adulto;
III. Sites de drogas;
IV. Sites de educação;
V. Sites de entretenimento;
VI. Sites de jogos;
VII. Sites de governo;
VIII. Sites de saúde;
IX. Sites de Tecnologia da Informação;
X. Sites de comunicação na Internet;
XI. Sites de pesquisa de emprego;
XII. Sites de notícias e mídia;
XIII. Sites de religião;
XIV. Sites de compras;
XV. Sites de viagens;
XVI. Sites de violência;
XVII. Sites de rádio e tv pela internet, telefonia pela internet e streaming de media;
XVIII. Sites de compartilhamento de arquivos ponto-a-ponto (P2P);
XIX. Sites de downloads de freeware ou software;
XX. Sites de mensagens instantâneas;
XXI. Sites de phising, keyloggers, redes de bots, websites maliciosos, softwares potencialmente indesejados e spyware;
XXII. Sites de conteúdo potencialmente perigoso, exposição elevada e explorações emergentes;

o) Deve ser capaz de operar em modo de monitoramento e verificar o impacto ao usuário final antes de habilitar a proteção;

p) Deve ser capaz de registrar log detalhado de acesso dos usuários com, no mínimo, as seguintes informações:

I. Tipo do evento (Visita ou Download)
II. Hora do Evento
III. Domínio
IV. URL
V. Classificação do Domínio
VI. Fator de Ameaça do Site
VII. Lista de Autorização
VIII. Ação
IX. Modo de Monitoramento (sim ou não)

q) Deve prevenir que o usuário faça alterações nos arquivos, registros e desinstale os plugins dos browsers;

r) Possibilidade de adicionar os endereços IP's internos de forma que o plugin não classifique ou tome ação nos sites internos (Intranet, por exemplo);

**4. Módulo de Proteção de Email**

a) Servidores Microsoft Exchange Server;

b) Compativeis com as plataformas Windows 2003, Windows 2008 e Windows 2012 ou superior;

c) Suporte a Exchange 2010 SP2 e Exchange 2013 ou superior;

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

I. Limpar o arquivo infectado e entregá-lo limpo para o(s) destinatário(s);
II. Gravar o arquivo infectado na área de segurança (quarentena) e não entregá-lo para o(s) destinatário(s);
III. Gerar notificações e alertas e entregar o arquivo para o(s) destinatário(s);

e) Rastreamento manual às pastas do Exchange, com opção de limpeza;

f) Programação de rastreamentos automáticos do Exchange com as seguintes opções:

I. Escopo: Todas as pastas locais, ou pastas específicas
II. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena) Frequência: Horária, diária, semanal, mensal;

g) Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo usuário, com limite de tamanho opcional;

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

i) Identificação de remetente e destinatário das mensagens;

j) Permitir bloqueios baseados nos seguintes critérios:

I. Tipo de arquivo;
II. Nome do arquivo;
III. Tamanho do arquivo;

k) Permitir a instalação em ambientes em Cluster Microsoft;

l) Capacidade de filtragem de conteúdo por categorias como: Sexo, Drogas, entre outros;

**5. Módulo de Controle de Dispositivos**

a) Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, Ipods, Dispositivos Bluetooth, DVDs, e CDS regraváveis;

b) Deve permitir a configuração dos dispositivos nos modos:

I. Bloqueio, ou;
II. Somente Leitura;

c) Deve classificar os dispositivos removíveis em 3 categorias:

I. Gerenciado;
II. Ingerenciável (Exemplo: Bateria de Notebooks);
III. Não Gerenciado;

d) Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:

I. Tipo de BUS;
II. Classe do Dispotivo (Device Class)
III. ID do fabricante (Vendor ID)
IV. ID do produto (Product ID)

e) Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:

I. Tipo de BUS
II. Se o sistema de arquivo é passível de escrita;
III. Se o sitema de arquivo é somente leitura;
IV. Tipo de Sistema de Arquivo
V. Nome do Sistema de Arquivo;
VI. Número de Série do Sistema de Arquivo;

f) Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado a rede do orgão libera o uso de pen-drive);

**6. Módulo de Gerência**

a) A gerência deve ser centralizada e suportar a gestão de todos os módulos listados neste Projeto Básico;

I. Não serão aceitas soluções que possuam mais de uma console de gestão;

b) Deve suportar a instalação nos seguintes sistemas operacionais:

I. Windows Server 2012 Release 2;
II. Windows Server 2012;
III. Windows Server 2008 Service Pack 2 (SP2) Standard, Enterprise ou Datacenter;
IV. Windows Server 2008 R2 Standard, Enterprise ou Datacenter;

V. Windows Server 2003 Service Pack 2 Standard, Enterprise ou Datacenter;
VI. Windows Server 2003;

c) A arquitetura dos Sistemas Operacionais deve ser 64-bits;

d) Deve suportar a instalação em Cluster Microsoft;

e) Deve suportar Ipv4 e Ipv6;

f) Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:

I. Vmware ESX;
II. Citrix Xen Server;
III. Microsoft Hyper-V;

g) Deve possuir suporte a base de dados:

I. SQL Server 2012 ou superior
II. SQL Server 2008 SP1/SP2/R2 Standard ou Enterprise
III. SQL Server 2005 SP3 Standard ou Enterprise

h) Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;

i) A console de gerência deve ser acessada via WEB;

j) Deve possuir compatibilidade com os seguintes browsers:

I. Google Chrome;
II. Firefox;
III. Internet Explorer 7 ou superior;
IV. Safari 6.0 ou superior;

k) Deve ser possível segregar a instalação da solução em:

I. Servidor Console Central
II. Servidor Base de Dados
III. Servidor de Interação com os Agentes
IV. Agentes Distribuidores de Vacina

l) Deve suportar o uso do SQL Server em ambientes SAN;

m) Permitir a instalação dos Módulos da Solução a partir de um único servidor;

n) Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota;

o) Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE nesta contratação presente ou futura;

p) Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local;

q) Visualização das características básicas de hardware das máquinas;

r) Integração e Importação automática da estrutura de domínios do Active Directory já existentes na rede local;

s) Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede;

t) Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;

u) Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede;

v) Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;

w) Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente;

x) Permitir a criação de grupos virtuais através de "TAGs";

y) Permitir aplicar as "TAGs" nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;

z) Deve possuir capacidade analítica de verificar a postura dos ativos e identificar quais destes estão em risco;

aa) Deve integrar com o módulo de controle de aplicação e módulo de prevenção de intrusos para informar dados de aplicações executadas nas estações;

bb) Deve ser capaz de identificar quais aplicações foram executadas no ambiente;

cc) A partir da identificação das aplicações executadas, a ferramenta deverá ser capaz de identificar quais aplicações impõe risco ao ambiente;

dd) Deve priorizar áreas de risco e informar as estações que necessitam de atualização;

ee) Forçar a configuração determinada no servidor para os clientes;

I. Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente;
II. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS;

ff) Forçar a instalação dos Módulos da Solução nos clientes;

I. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido;

gg) Customização dos relatórios gráficos gerados;

hh) Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF e XML

ii) Geração de relatórios que contenham as seguintes informações:

I. Máquinas com a lista de definições de vírus desatualizada;
II. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;

III. Os vírus que mais foram detectados;
IV. As máquinas que mais sofreram infecções em um determinado período de tempo;
V. Os usuários que mais sofreram infecções em um determinado período de tempo;
VI. Gerenciamento de todos os módulos da suíte;

jj) Possuir dashboards no gerenciamento da solução;

kk) Deve ser capaz de identificar e apresentar uma visibilidade sobre quais estações executaram um determinado arquivo (executável);

ll) Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:

I. Cobertura da proteção de Navegação Segura;
II. Relatório dos últimos 30 dias da detecção de códigos maliciosos;
III. Top 10 Computadores com Infecções;
IV. Top 10 Computadores com Sites bloqueados pela politica;
V. Resumo das ações tomadas nos últimos 30 dias no que se refere a Filtro de Navegação na web;
VI. Resumo dos tipos de sites acessados nos últimos 30 dias no que se refere a Filtro de Navegação Segura;

mm) Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota;

nn) Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;

oo) Ter a capacidade de gerar registros/logs para auditoria;

pp) A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento;

qq) A solução de gerenciamento deve permitir acesso a sua console via web;

rr) Implementação de Dashboard com medição do nível de atualização do ambiente e o nível de cumprimento de política de segurança previamente definida.

**6.2. Item 2 - Solução de segurança de endpoints para servidores virtuais com licenciamento, instalação, capacitação e suporte: McAfee MOVE antivírus, com ePO, TIE, GTI file reputation e HIPS.**

**1. Características Gerais**

a) Deve ser uma solução específica e otimizada para funcionar e interoperar com ambiente virtual;

b) Deve eliminar o uso de agentes para as seguintes tecnologias:

I. Antivirus
II. Firewall

c) Deve ter total integração com a API da Vmware – Vshield Endpoint e/ou Vmware NSX

**2. Características do Sofware**

a) Deve suportar análise no momento que um arquivo é acessado;

b) Deverá suportar análise de todos os arquivos em uma máquina virtual (scan sob demanda) permitindo agendar a frequência das verificações;

c) Deverá suportar, no mínimo, as seguintes plataformas de virtualização:

I. Microsoft 2012 Hyper-V;
II. Microsoft 2008 Hyper-V;
III. Vmware vSphere;
IV. Vmware View;
V. Vmware Horizon View;
VI. Citrix Xen Server;
VII. Citrix Xen Desktop;

d) Deve suportar os seguintes sistemas em máquinas "Guest"

I. Windows 2012 R2 (64 bits) ou superior;
II. Windows 2012;
III. Windows 2008 R2 (64 bits);
IV. Windows 2008 (32 bits);
V. Windows 2003 R2 (32 bits);
VI. Windows Vista (32/64 bits);
VII. Windows 7 (32/64 bits);
VIII. Windows 8 (32/64 bits);
IX. Windows 8.1 (32/64 bits) ou superior;

e) Através da integração com o Vmware vSphere deve ser possível descobrir e importar as instâncias de máquinas virtuais paradas ou em execução;

f) A solução deverá contar com um cache que permita otimizar os recursos evitando analisar arquivos que já tenham sido analisados anteriormente e não tenha sofrido alterações.

I. Este cache deve ser local (guest machine) quanto centralizado em cada analisador (scanner);
II. O tamanho do cache deve ser configurável;

g) Deve ser possível configurar a quantidade de análise simultâneas que deve ser executada em cada analisador;

h) Deve ser possível configurar o tipo de arquivo a ser analisado;

i) Deve manter uma quarentena local em cada servidor ou em um compartilhamento remoto em caso de detecção de ameaça;

j) Como resultado da ação deve ser possível manter o arquivo ou eliminá-lo;

k) Deve ser capaz de analisar unidades de rede;

l) Deve suportar vMotion;

m) Deve ser possível criar uma imagem base de scan e a partir dela gerar apenas diferencial;

n) Deve ser possível criar analises específicas com base em:

I. Grupos;
II. Resource Pools;
III. Maquinas Virtuais específicas;

o) Toda e qualquer ameaça encontrada deve ser informada na console de gestão centralizada;

p) Deve permitir a criação de regras de firewall como forma de isolar certos recursos do Data Center Virtual e protegê-los de ameaças provenientes de outros recursos dentro da mesma infraestrutura;

q) Deve permitir criação de regras de isolamento baseadas em:

I. i. Detalhes do Isolamento;
II. ii. Acesso Entrada;
III. iii. Acesso Saída;

r) Deve permitir a criação de regras de firewall baseadas em:

I. Origem;
II. Destino;
III. Serviços;
IV. Ação;
V. Registro de Evento;

s) Deve prover um conjunto de regras pré-configuradas;

t) Deve ser possível realizar troubleshoot de problemas de comunicação através de registro dos eventos em um arquivo;

u) Deve permitir a configuração de regras de firewall através de endereços MAC;

v) Deve ser possível criar uma lista de exclusão de máquinas guest que serão excluídas da proteção;

**3. Características de Arquitetura**

a) A solução deve possuir gestão única através da mesma console de gestão do Módulo de Gerência;

b) Deverá permitir a instalação e criação de analisadores em alta disponibilidade;

c) Deverá suportar analisadores em alta disponibilidade com possibilidade de instalá-lo fora do cluster existente;

d) Não deve requerer reinício do Hypervisor durante a instalação da solução;

e) O analisador deve possuir comunicação com o Centro de Inteligência do fabricante para classificar arquivos suspeitos;

f) Para o caso de instalação em múltiplos hypervisors, o instalador deve prover um meio automatizado de execução;

**4. Características de Gestão**

a) A console de gestão deve permitir a visualização das máquinas virtuais designadas para cada analisador;

b) Deverá permitir a configuração centralizada das análises contra artefatos maliciosos;

c) Deve ser possível criar uma política por máquina virtual;

d) A solução deve permitir o download de atualizações de vacina e engines de maneira periódica e automática e aplicá-las aos componentes da solução;

e) Deve ser possível elencar a quantidade de servidor de análise necessárias para a proteção do ambiente de maneira automática;

f) Não deve possuir diferença de políticas entre hypervisor distintos (Hyper-V e Vmware);

g) Deve ser possível criar políticas diferenciadas para análise sob demanda e análise em tempo de acesso;

h) Deve ser possível criar políticas para análise de arquivos em drives de rede;

i) Deve integrar de maneira nativa com a solução de base de dados local de ameaças.

**Solução de Base de Dados Local de Ameaças**

a) Da Arquitetura

I. A solução deve ser compreendida nos seguintes módulos e fornecida juntamente com os itens 1 e 2:

1. Servidor de Orquestração e Base de Dados

2. Agentes

II. O servidor de orquestração deverá habilitar a troca de informação de ameaças entre os itens 1 e 2, compreendendo:

1. Solução de Proteção de Endpoints para estações de trabalho e servidores físicos;

2. Solução de Proteção de Endpoints para servidores virtuais.

III. A instalação do componente central deverá habilitar um protocolo de troca de informações de ameaças que permita o intercambio de informações entre soluções do mesmo fabricante e de fabricantes terceiros;

IV. A troca de informação de ameaças deve ser dar por meio de protocolo performático;

V. O servidor de orquestração deve permitir a instalação em modo centralizado ou em modo descentralizado, permitindo que localidades remotas possuam um servidor local;

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

b) Da Solução

I. A solução deve possuir capacidade de criar uma reputação local através da catalogação de todos os executáveis existentes no ambiente;

## PROJETO BÁSICO

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

1. Reputaçao Local
2. Reputação do Centro de Inteligência
3. 
4. do Fabricante

III. Ao catalogar um arquivo, a solução deve apresentar, no mínimo, as seguintes informações sobre o mesmo:

1. Nome do arquivo
2. Caminho do arquivo
3. Hash SHA-1
4. Hash MD5
5. Hash 256
6. Primeira visualização do arquivo na rede
7. Última visualização do arquivo na rede
8. Tamanho do arquivo
9. Data de compilação
10. Se o mesmo consta no Adicionar/Remover Programas
11. Se está registrado como serviço
12. Se está registrado para ser executado automaticamente
13. Tipo de compactador
14. Se é arquivo do sistema
15. Se foi executado a partir do cmd.exe
16. Se tem entrada no menu iniciar
17. Se foi executado a partir de uma mídia removível
18. Se foi executado a partir da raiz da unidade do sistema

IV. Caso o arquivo tenha como origem a Internet, a solução deverá ser capaz de informar a partir de qual URL o arquivo foi obtido e a reputação desta última;

V. Deve ser possível realizar uma pesquisa do arquivo em base de conhecimento de terceiros (Exemplo: VirusTotal);

VI. Após análise o administrador deve ter a possibilidade de:

1. Rastrear em quais estações o arquivo foi executado;
2. Identificar o país de origem do arquivo;
3. Identificar o arquivo como confiável;
4. Identificar o arquivo como desconhecido;

5. Identificar o arquivo como malicioso

VII. Deve ser capaz de analisar o certificado associado ao arquivo;

VIII. Deve ser capaz de identificar o certificado associado como confiável ou malicioso;

IX. Para minimizar o impacto a solução deve ter a capacidade de ser ativada no modo de observação;

X. Deve ser possível configurar o limiar mínimo para bloqueio de arquivos, variando entre:

1. Malicioso

2. Provavelmente malicioso;

3. Desconhecido

XI. Deve ser possível bloquear a execução de arquivos nunca antes visto no ambiente e informar o usuário por meio de mensagem customizada em Português.

XII. Deve ser capaz de identificar manualmente um arquivo como malicioso impedindo sua execução no ambiente;

XIII. Deve ser gerenciado pela mesma console proposta na Solução de Proteção de Endpoints.

## 7. DA EXECUÇÃO E DA GESTÃO DO OBJETO CONTRATADO

### 7.1 Modelo de execução e de gestão do objeto contratado

#### 7.1.1 Papeis e responsabilidades

| Papéis | Entidade | Responsabilidade |
|---|---|---|
| Equipe de Apoio à Contratação | TRT19 | Equipe responsável por subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes. |
| Equipe de Gestão da Contratação | TRT19 | Equipe composta pelo Gestor da Contratação, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares. |
| Fiscal Demandante da Contratação | TRT19 | Servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o objeto contratado |

| | | |
|---|---|---|
| | | quanto aos aspectos funcionais da solução. |
| Fiscal Técnico da Contratação | TRT19 | Servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar a contratação quanto aos aspectos técnicos da solução. |
| Fiscal Administrativo da Contratação | TRT19 | Servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar a contratação quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais. |
| Gestor da Contratação | TRT19 | Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão da Contratação, indicado por autoridade competente do órgão. |
| Preposto | Contratada | Funcionário representante da empresa contratada, responsável por acompanhar a execução da Contratação e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. |
| Responsável pela Solução | TRT19 | Servidor responsável pela implantação e manutenção da solução |

### 7.1.2 Dinâmica de Execução

1. **O prazo máximo para a entrega e instalação do software será de 5 dias úteis, contados a partir da data de envio da Nota de Empenho.**
2. **Não será celebrado contrato nesta ação.**
3. A vigência do objeto contratado terá início **da data de envio da Nota de Empenho** e se estenderá até o fim do prazo de garantia.
4. O prazo de garantia de 6 meses inicia-se após o recebimento definitivo do objeto da presente contratação.
5. Início da prestação dos serviços de suporte e atualização a contar do recebimento definitivo.
6. Na contagem dos prazos, excluir-se-á o dia de início e incluir-se-á o dia do vencimento.
7. A prorrogação do prazo de entrega poderá ser concedida em caráter excepcional e sem efeito suspensivo, devendo a Contratada encaminhá-lo por escrito ao órgão Contratante, com antecedência mínima de 01 (um) dia

do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada, em conformidade com o art. 57, §1.º, da Lei n.º 8.666/93.

### 7.1.3 Instrumentos de solicitação dos bens e/ou de serviços

1. A nota de empenho emitida é o instrumento que autoriza o fornecimento dos bens.

### 7.1.4 Garantia e Nível de Serviço (SLA)

1. O atendimento aos chamados deverá estar disponível de segunda-feira a sexta-feira, no horário das 7h às 18h, horário de Brasília. A abertura de chamados pelo Contratante será efetuada por correio eletrônico, por sistema de controle de chamados ou por telefone. A abertura de chamado poderá ocorrer em qualquer horário por email ou sistema de controle de chamados, por telefone apenas no horário mencionado. No caso de abertura de chamado fora do horário estipulado, a contagem do prazo para efeitos de SLA se dará no próximo dia útil.
2. A assistência técnica em garantia deve garantir o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).
3. O suporte técnico do fabricante deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes às plataformas de software e hardware (inclusive virtual) dos produtos.
4. Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, instalação de novas versões, patches e hotfixes, análise de dúvidas sobre melhores práticas de configuração, entre outros.
5. Os chamados de severidade ALTA (quando há indisponibilidade de uso da solução) deverão ser atendidos em até 02 (duas) horas após a abertura e deverão ser solucionados em até 24 (vinte e quatro) horas, contadas a partir da abertura do chamado.
6. Os chamados de severidade MÉDIA (quando há falha, simultânea ou não, de uma ou mais funcionalidades que não cause indisponibilidade, mas apresente problemas de funcionamento e/ou performance da solução) deverão ser atendidos em até 04 (quatro) horas após a abertura e deverão ser solucionados em até 48 (quarenta e oito) horas, contadas a partir da abertura do chamado.
7. Os chamados de severidade BAIXA (nível de severidade aplicado para instalação, configuração, atualização de versões e implementações de novas funcionalidades) deverão ser atendidos em até 06 (seis) horas após a abertura e deverão ser solucionados em até 72 (setenta e duas) horas, contados a partir da abertura do chamado.
8. Automaticamente e sem custos adicionais, deverá ser possível o acesso ao conteúdo mais recente dos produtos, funcionalidades adicionais e correções de produtos disponibilizadas pelo fabricante.

### 7.1.5 Mecanismos formais de comunicação

1. A forma de comunicação e acompanhamento da execução do objeto contratado se dará por meio de ofícios, e-mails ou chamados telefônicos. As notas fiscais e certidões poderão ser enviadas por e-mail ou entregues pessoalmente.

### 7.1.6 Estratégia de continuidade em eventual interrupção contratual

1. Evento 1: Interrupção contratual por problemas com a empresa vencedora do certame antes da entrega/instalação dos produtos
2. Ação de Contingência 1: Informar à Administração do Tribunal para aplicações das sanções previstas.
3. Responsável: Gestor da contratação.
4. Ação de Contingência 2: Iniciar os trabalhos para realização de uma nova contratação.
5. Responsável: Gestor da contratação.

### 7.1.7 Ações para transição e encerramento contratual

1. Ação: Realização de procedimentos para nova contratação.
2. Responsável: Gestor da contratação, Equipe de planejamento da contratação, Setor de Licitações e administração do Tribunal.
3. Data de Início: até 90 (noventa) dias antes do encerramento da contratação.
4. Data do Fim: até 30 (trinta) dias antes do encerramento da contratação.

### 7.1.8 Propriedade, sigilo e restrições

- Direito de Propriedade: Baseados na Lei nº 9.610 de 19 de fevereiro de 1998.
- Condição de Manutenção de Sigilo:

1. A CONTRATADA deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do Contratante ou de terceiros de que tomar conhecimento, em razão da execução do objeto desta contratação, devendo orientar seus empregados nesse sentido.
2. Os conhecimentos, dados e informações de propriedade do CONTRATANTE, tanto tecnológicos como administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto da contratação, constituem informação privilegiada e possuem caráter de confidencialidade.
3. Estas informações poderão ser utilizadas, só e exclusivamente, no cumprimento das cláusulas e condições estabelecidas neste Projeto Básico, sendo expressamente vedado à CONTRATADA:

   a) Utilizá-las para fins não previstos no instrumento contratual; e

   b) Repassá-las a terceiros e/ou empregados não vinculados diretamente à execução do objeto contratado.·

Restrição Adicional: São do CONTRATANTE todos os direitos de propriedade intelectual e direitos autorais associados ao material produzido em suas dependências.

### 7.1.10 Qualificação técnica/profissional

1. Não se aplica, pois será mantido o fornecedor atual.

### 7.1.11 Descumprimento das Obrigações Contratuais

1. A disciplina das infrações e sanções administrativas aplicáveis no curso da licitação e da contratação é aquela prevista no Edital, em conformidade com as normas praticadas neste Tribunal e na legislação pertinente.
2. Garantida ampla e prévia defesa, nos termos do art. 87 da Lei n.º 8.666/93, à CONTRATADA poderão ser aplicadas cumulativamente as penalidades permitidas em lei e as constantes deste instrumento, que são:
3. Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízo significativos ao objeto da contratação;
4. Multa moratória de 0,5% (meio por cento) por dia de atraso, calculada sobre o valor total da contratação, cabível nos casos de atraso injustificado de até 30 (trinta) dias no cumprimento dos prazos previstos neste instrumento para os compromissos assumidos.
5. O atraso injustificado por período superior a 30 (trinta) dias caracterizará a inexecução total da contratação;
6. Multa por inexecução contratual parcial de até 15% (quinze por cento), calculada hipóteses de inexecução contratual;
7. Multa rescisória de 20% (vinte por cento) do valor total da contratação, pela inexecução total da contratação;
8. Impedimento de licitar e de contratar com a Administração Pública, nos termos do art. 7.º da Lei n.º 10.520/2002;
9. As sanções de suspensão do direito de licitar e contratar com a Administração Pública poderão ser aplicadas cumulativamente com a de multa.
10. Em caso de não-atendimento ao acordo de nível de serviço (SLA) especificado, pelo período de 03 (três) meses consecutivos ou por 06 (meses) não consecutivos, será caracterizada a inexecução parcial da contratação.
11. Em caso de não cumprimento dos itens de Severidade Alta, Média e Baixa, registrados no acordo de nível de serviço (SLA), especificado no item 3.1.4, será aplicado uma multa de 20%, 15% e 10%, respectivamente aos itens supracitados, no valor da mensalidade, para cada evento registrado no respectivo mês. Devendo a cobrança da multa ser aplicada no pagamento do mês imediatamente subsequente.
12. As penalidades pecuniárias descritas neste documento poderão ser descontadas dos pagamentos devidos pelo CONTRATANTE, conforme permissibilidade contida na Lei n.º 8.666/93.

13. Serão considerados injustificados os atrasos não comunicados contemporaneamente à ocorrência do fato impeditivo do cumprimento da obrigação e indevidamente fundamentados, ressalvados os casos previstos em lei.
14. Não havendo prejuízo para o CONTRATANTE, as penalidades pecuniárias referidas neste item poderão ser relevadas ou transformadas em outras de menor sanção, a seu critério.

### 7.2 Requisitos Técnicos Específicos

7.2.1 Console de gerenciamento: Gerência centralizada e integrada, a partir de uma única console para todo o parque instalado, para as ferramentas integradas de segurança em estações de trabalho e servidores, de onde seja possível manter a proteção atualizada, gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle. Deve prover uma console web de gerenciamento centralizado acessado via HTTPS.

7.2.2 Serviço de instalação será realizado por operação assistida (on-site) em cada regional.

7.2.3 Clientes para Sistemas Operacionais Windows, Linux (Red Hat, CentOS, Oracle Linux, Ubuntu) e OS X.

7.2.4 Caso necessárias, Windows Client Access License (CAL) devem ser fornecidas.

## 8. RECEBIMENTO E PAGAMENTO DOS SERVIÇOS

### 8.1 Forma de Recebimento e Avaliação da Qualidade

8.1.1 Local de entrega: Os itens deverão ser entregues e instalados no TRT da 19ª Região, situado à Avenida da Paz, 2076, Centro, Maceió/AL.

8.1.2 Os recebimentos provisório e definitivo serão emitidos da seguinte forma:

- Recebimento Provisório – imediatamente após a entrega e instalação dos bens;
- Recebimento Definitivo – após realização de testes pelo CONTRATANTE em conjunto com a CONTRATADA no prazo máximo de 15 (quinze) dias corridos, contados do recebimento provisório, pela equipe de gestão da contratação, depois de verificadas a qualidade e a quantidade do material.

### 8.2 Condições de Pagamento

8.2.1 O pagamento será mensal e a primeira parcela será paga após 30 (trinta) dias corridos do recebimento definitivo.

8.2.2 A CONTRATADA apresentará Nota Fiscal ou Fatura, em Reais, relativa aos objetos contratados à comissão designada para receber os bens que, atestando-a (recebimento definitivo), a encaminhará para pagamento mediante emissão de Ordem Bancária.

8.2.3 A CONTRATADA deverá fornecer as seguintes informações para fins de pagamento: nome e código do banco e agência bancária e número da conta corrente.

8.2.4 A unidade responsável pelo pagamento verificará a regularidade fiscal da contratada quanto à: Certidão Conjunta de Débitos Relativos a Tributos e à Dívida Ativa da União, Certidão Negativa de Débitos Trabalhista, Certidão Negativa de Débito com o INSS e Certificado de Regularidade de Situação do FGTS e consulta ao CADIN.

8.2.5 Caso a nota fiscal seja apresentada com erro, será devolvida para retificação e reapresentação, acrescentando-se, no prazo aqui fixado os dias que se passarem entre a data da devolução e a reapresentação; assim como na hipótese de inadimplência nas certidões tratadas no item anterior.

8.2.6 Observar-se-á, ainda, se o CNPJ apresentado na nota fiscal é o mesmo constante dos documentos habilitatórios e proposta apresentada.

8.2.7 Será efetuada por este Tribunal a retenção na fonte dos tributos e contribuições elencados na legislação em vigor, tais como, IR, CSLL, COFINS e PIS/PASEP.

8.2.8 A retenção dos tributos não será efetuada caso o licitante apresente juntamente com a Nota Fiscal a comprovação de que a mesma é optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES.

8.2.9 A Nota Fiscal e os documentos exigidos no Edital, para fins de liquidação e pagamento das despesas, deverão ser entregues exclusivamente ao gestor da contratação.

8.2.10 Não será efetuado qualquer pagamento à contratada enquanto houver pendência de liquidação da obrigação financeira em virtude de inadimplência contratual. Esse fato não será gerador de direito a reajustamento de preços ou atualização monetária.

8.2.11 O pagamento fica vinculado, ainda à comprovação do recolhimento do ISS referente aos serviços, junto ao órgão arrecadador do Município, caso exista.

8.2.12 Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração do contratante, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmula:

$$I = \frac{\frac{TX}{100}}{365} \text{ e } EM = I * N * VP$$

## 9. TRANSFERÊNCIA DE CONHECIMENTO

9.1. Não se aplica, pois será mantida e solução atual.

# PROJETO BÁSICO

## 10. ESTIMATIVAS DA CONTRATAÇÃO

### 10.1. Valor Estimado da Contratação

| | | | | | Pesquisa de preços TRT13 | | |
|---|---|---|---|---|---|---|---|
| | | | | Orçamento Netsafe | Orçamento Xsite* | Orçamento AboutNet* | Orçamento Fasthelp* |
| Item | Descrição | Classificação da Despesa | Quant. | Valor Unitário mensal | Valor Unitário mensal | Valor Unitário mensal | Valor Unitário mensal |
| 1 | Solução de segurança de endpoints para estações e servidores físicos com licenciamento,instalação, capacitação e suporte: McAfee Endpoint Protection Suite multiplataforma com ePO, TIE, Controle de dispositivos, firewall ePO, TIE, Controle de dispositivos, firewall integrado, HIPS, antimalware, proteção de email controle de web com filtragem de URL e pesquisa segura. | 33904006 LOCACAO DE SOFTWARE | 1250 | R$ 1,77 | R$ 4,94 | R$ 4,90 | R$ 5,04 |
| 2 | Solução de segurança de endpoints para servidores virtuais com licenciamento, instalação, capacitação e suporte: McAfee MOVE antivirus, com ePO, TIE, GTI file reputation e HIPS.com ePO, TIE, GTI file reputation e HIPS. | | 80 | R$ 2,59 | R$ 8,31 | R$ 8,39 | R$ 5,62 |
| | | | ***VALOR TOTAL MENSAL*** | R$ 2.419,70 | R$ 6.838,14 | R$ 6.800,38 | R$ 6.755,03 |
| | | | ***VALOR TOTAL 6 MESES*** | R$ 14.518,20 | R$ 41.028,83 | R$ 40.802,30 | R$ 40.530,15 |

* Os valores nas propostas estão unitários para 48 meses. Para obter-se o valor mensal, foi feita a divisão do valor por 48.

| Fornecedores | CNPJ/CPF | Contatos |
|---|---|---|
| NETSAFE CORP | 03.476.184/0002-30 | Nome: Norberto Lucena<br>Telefone: (81) 81 99608-7776<br>E-mail: norberto.lucena@netsafecorp.com.br |
| Centro de Pesquisas em Informática Eireli (XSITE) | 40.584.096/0001-05 | Nome: João Gualberto Rizzo Araujo<br>Telefone: (71)3018-7284<br>E-mail: jgra@xsite.com.br |
| AboutNet Informática Ltda - EPP | 07.751.724/0001-16 | Nome: Álvaro Alves<br>Telefone: 11 5612 8200<br>E-mail: |
| FAST HELP INFORMÁTICA LTDA | 05.889.039/0001-25 | Nome: Denis Silva<br>Telefone: (61) 3363-8636<br>E-mail: comercial@fasthelp.com.br |

# PROJETO BÁSICO

## 11. DOTAÇÃO ORÇAMENTÁRIA

11.1. As despesas resultantes desta licitação correrão à conta das dotações orçamentárias mediante verba a ser informada quando da contratação do objeto.

# PROJETO BÁSICO

## 12. MODELOS (TEMPLATES)

12.1. **Modelo de Termo de Recebimento Provisório**:

Declaro o recebimento provisório dos itens abaixo relacionados, fornecidos pela Empresa _____, mediante nota fiscal _____ emitida para o TRT da 19ª Região.

| ITEM | DESCRIÇÃO | QUANT. |
|---|---|---|
| 1 | Solução de segurança de endpoints para estações e servidores físicos com licenciamento, instalação, capacitação e suporte: McAfee Endpoint Protection Suite multiplataforma com ePO, TIE, Controle de dispositivos, firewall integrado, HIPS, antimalware, proteção de email, controle de web com filtragem de URL e pesquisa segura | |
| 2 | Solução de segurança de endpoints para servidores virtuais com licenciamento, instalação, capacitação e suporte: McAfee MOVE antivirus, com ePO, TIE, GTI *file reputation* e HIPS | |

Local e data

_____
Gestor da contratação

_____
Fiscal Demandante

_____
Fiscal Técnico

_____
Fiscal Administrativo

# PROJETO BÁSICO

12.2. **Modelo de Termo de Recebimento Definitivo**:

Declaro o recebimento definitivo dos itens abaixo relacionados, fornecidos pela Empresa _____, mediante nota fiscal _____ emitida para o TRT da 19ª Região.

| ITEM | DESCRIÇÃO | QUANT. |
|---|---|---|
| 1 | Solução de segurança de endpoints para estações e servidores físicos com licenciamento, instalação, capacitação e suporte: McAfee Endpoint Protection Suite multiplataforma com ePO, TIE, Controle de dispositivos, firewall integrado, HIPS, antimalware, proteção de email, controle de web com filtragem de URL e pesquisa segura | |
| 2 | Solução de segurança de endpoints para servidores virtuais com licenciamento, instalação, capacitação e suporte: McAfee MOVE antivirus, com ePO, TIE, GTI *file reputation* e HIPS | |

Local e data

_____
Gestor da contratação

_____
Fiscal Demandante

_____
Fiscal Técnico

_____
Fiscal Administrativo

## 13. GENERALIDADES

13.1. Os dados do TRT 19ª Região: CNPJ: 35.734.318/0001-80; UASG: 080022.

Maceió, 4 de junho de 2021.

| | | |
|---|---|---|
| MANOEL ABREU<br>Integrante Requisitante | ULISSES SILVA MELO<br>Integrante Técnico | ANDRE LUIZ CUNHA<br>Integrante Administrativo |

MANOEL MESSIAS FEITOZA
Secretário da SETIC