TRIBUNAL REGIONAL ELEITORAL DA PARAÍBA
Avenida Princesa Isabel, 201 - Bairro Centro - CEP 58020-911 - João Pessoa - PB - http://www.tre-pb.jus.br

Contratação - Estudos Preliminares IN 1/2018TREPB nº 2/2022 - NSI

ESTUDO PRELIMINAR DA CONTRATAÇÃO

Caracterização da Demanda

1. Descrição da Solução de TIC a ser contratada

Participação em Registro de preço conduzido pelo TSE para contratação de subscrições de solução de antimalware avançada com EDR e XDR para estações e servidores, serviço de instalação e transferência de conhecimento, com pagamento anual, pelo período do de 60 meses.

1.1. DFD(s) que compõe(m) a solução de TIC

DFD que compõe a solução de TIC descrito neste estudo: 1123444.

2. Equipe de planejamento da contratação

Integrante	Nome	Ramal	E-mail	Setor
Demandante	*Felipe Cavalcanti Alves*	1330	felipe.alves@tre-pb.jus.br	NSI
Administrativo	Soraya Cavalcanti Bezerra Norat	1276	sorayanorat@tre-pb.jus.br	SECONT
Técnico	Pedro de Figueiredo Lima Neto	1338	pedro.lima@tre-pb.jus.br	SEINF
Técnico	Airton Alves de Medeiros Júnior	1414	airton.alves@tre-pb.jus.br	SEINF

3. Necessidade da contratação

Garantir proteção contra vírus de computador e ameaças conhecidas, seja nos desktops físicos e virtuais, quanto nos servidores de rede do tribunal.

4. Alinhamento estratégico

Objetivo 4 do PEI: Aperfeiçoar a comunicação e a informação.

Objetivo 8 do PEI: Aperfeiçoar a governança e gestão.

Seção I - Análise da Viabilidade da Contratação

5. Requisitos da contratação

O presente estudo objetiva a contratação de subscrições de solução de antimalware avançada com EDR e XDR para estações de trabalho e servidores, físicos ou virtuais, para atender as necessidades de segurança da informação do Tribunal Regional Eleitoral da Paraíba.

5.1 Necessidades do negócio

Necessidade: Proteção avançada antimalware para estações de trabalho e servidores de rede.

Necessidade: Proteção contra execução de aplicações maliciosas.

Necessidade: Análise e bloqueio da execução de aplicações baseada em comportamento.

Necessidade: Monitoramento de atividades de criptografia de arquivos para evitar ataques de ransomware.

Necessidade: Proteção contra ataques direcionados e 0Day.

Necessidade: Proteção para a solução de correio eletrônico do TSE com capacidade de atendimento ao tráfego de e-mail gerado.

Ator(es) Envolvido(s): STIC.

5.2 Requisitos Tecnológicos e Não Funcionais

5.2.1. Requisitos Tecnológicos

5.2.1.1 Requisitos Tecnológicos Gerais

Aquisição de soluções de seguranças do tipo Solução de Antivírus, incluindo licenciamento, serviços de instalação, suporte técnico, repasse de conhecimento, garantia e atualização por 60 (sessenta) meses.

Especificações Técnicas e Requisitos Gerais Mínimos da Solução de Antivírus: Proteção contra execução de aplicações maliciosas (Application Control) ou similares.

Proteção Web para verificação de sites, inclusive tráfego SSL, e downloads a fim de impedir o acesso e mitigar o risco de infecção por pragas virtuais.

A solução deve se auto proteger contra ataques aos seus serviços e processos e deve ter a capacidade de implementar a funcionalidade de "Machine Learning" (aprendizado de máquina).

A solução deve contemplar proteção contra ataques: direcionados e suas variantes, 0Day (dia zero), vulnerabilidades desconhecidas ou novas, tais como as que possam causar estouro de buffer, ataques iniciados a partir de mídias removíveis, proteção contra BOT's e variantes.

Possuir análise de comportamentos suspeitos para detecção, bloqueio e eliminação das aplicações e ameaças desconhecidas. Possuir análise Comportamental

(Behavioral Analysis) ou similar.

Monitoramento de atividades de criptografia de arquivos para evitar ataques de ransonware ou similar.

Mitigação da Exploração de Memória (Memory Exploit Mitigation) ou similar.

A solução deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de 0Day (dia zero), mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades.

A solução deve ter a capacidade de receber instruções de comando contra ataques de APT (Ameaça Persistente Avançada) ou similar, sem a necessidade de interpretação pelo gerenciador do endpoint, possibilitando ações mais rápidas, assertivas e minimizando falsos positivos.

A solução deve ser capaz de visualizar toda a cadeia de ataque, permitindo analisar a causa raiz e identificar as ameaças. Capacidade de identificar e bloquear a origem da infecção informando nome ou IP da origem, a fim de evitar a propagação pela rede.

Capacidade de limitar o acesso dos sistemas e aplicativos a recursos do sistema operacional, como chaves do registro e pastas e arquivos, em casos de falha, permitir a limpeza de chaves e pastas.

Possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do S.O. e aplicações terceiras.

Possuir a capacidade de detectar mudanças no estado de portas em sistemas operacionais Linux. Possuir a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e, customização de XML para criação de regras avançadas. Implementar a proteção contra acesso a websites ou URLs consideradas maliciosas, de baixa reputação ou não categorizadas.

5.2.1.2 Requisitos Tecnológicos item 1 "Solução de segurança de EndPoint (desktops), com EDR e Sandbox , com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses"

Proteção avançada antimalware para estações de trabalho.

Proteção e verificação nas mensagens de e-mail a fim de verificar e-mails recebidos, enviados e seus anexos.

A solução deverá ser compatível com sistemas operacionais: Windows 7 (32 e 64 bits) e superiores; Linux (Red Hat e suas variantes, Debian e suas variantes, Ubuntu e suas variantes) nas versões (32 e 64 bits); e MacOS (OS X 10.7 e superiores) nas versões (32 e 64 bits).

A solução deverá prover detecção e proteção em múltiplas camadas para verificação de malware e/ou códigos maliciosos.

Permitir verificação de vírus em recursos mapeados de rede solicitando senha.

Possuir funcionalidades, inclusive recursivo em vários níveis, que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados.

Detecção e remoção de vírus de macro.

Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede.

A solução deve ser capaz de identificar e bloquear informações independente do meio de transmissão.

A solução deverá permitir configuração de SSL/TLS para autenticação.

5.2.1.3 Requisitos Tecnológicos item 2 "Solução de segurança de EndPoint (desktops), com XDR e Sandbox , com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses"

A solução e suas funcionalidades deverão funcionar com agente único a ser instalado em servidores físicos e virtuais, a fim de diminuir o impacto aos sistemas e aplicações.

A solução deve possuir funcionalidades de otimização de verificação (escaneamento) em ambientes virtuais. A solução deve permitir visualizar máquinas físicas e virtuais, possibilitando aplicar regras específicas para as máquinas virtuais.

A solução deve ser compatível com, no mínimo, os seguintes sistemas operacionais: Windows Server 2003 ou superiores (32 e 64 bits); Linux Red Hat e suas variantes, CentOs, Debian e suas variantes nas versões (32 e 64 bits).

Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host. Proteger de forma automática e transparente contra brechas de segurança descobertas interrompendo somente o tráfego malicioso. Possuir a capacidade de detectar e bloquear ataques em aplicações web tais como: SQL Injection e Cross-Site Scripting dentre outros.

O software de proteção deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", assim como, implementar a funcionalidade de "virtual patching" ou qualquer outra técnica para blindagem de sistemas e aplicações contra exploração de vulnerabilidades conhecidas.

Implementar a customização avançada e criação de novas regras de proteção de aplicações web, permitindo proteger contra vulnerabilidades específicas de sistemas web do Ministério da Economia, inclusive sistemas legados.

Operar como firewall de host statefull bidirecional, monitorando as comunicações nos servidores protegidos.

Possuir a capacidade de controlar o tráfego baseado no Endereço MAC, Frame Types, Tipos de Protocolos, Endereços IP e intervalo de portas.

Permitir que as regras de Firewall executem as seguintes ações, ou equivalentes: Allow, Log Only, bypass, force allow, deny. Permitir limitar o número de conexões entrantes e de saídí a de um determinado IP de origem. Possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do S.O. e demais aplicações.

Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do S.O. e demais aplicações, recomendando ações para blindagem de vulnerabilidades existentes no S.O. e aplicações.

Possuir a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão.

Permitir que a opção de detecção e bloqueio seja implementada de forma global (todas as regras) ou apenas para uma regra ou grupos de regras.

Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, os seguintes sistemas operacionais e aplicações:

I - Windows Server 2003 ou superiores (32 e 64 bits);

II - Linux Red Hat e suas variantes, CentOs, Debian e suas variantes nas versões (32 e 64 bits);

III - Aplicações como: Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Postgree, MySQL Server e suas variantes, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Edge, Google Chrome, Safari, Web Server Apache, Tomcat, NGinx, Joomla, Plone, Wordpress, JBoss, Jenkins, OpenShift, Rancher e Docker.

A solução deverá suportar a tecnologia hiperconvergente Nutanix.

Possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque.

Possibilitar a criação de regras customizadas, para proteger aplicações desenvolvidas pela Justiça Eleitoral.

Implementar a inspeção de tráfego incoming SSL. Bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede.

Permitir que as regras de IPS atuem detectando ou bloqueando os eventos que as violem, de modo que o administrador possa decidir qual ação deva ser tomada.

Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLAN's ou Switches.

Detectar ameaças avançadas no ambiente cibernético.

Corrigir falhas antes que o erro aconteça.

Monitorar continuamente os endpoints, quer estejam online ou offline.

Armazenar eventos e incidentes de malwares no endpoint.

Possuir capacidade de resposta em tempo real.

Promover a unificação das informações dos endpoints.

Dar maior visibilidade do ambiente de TI.

Integrar-se com as demais soluções de segurança.

Usar whitelists e blacklists.

5.2.1.3 Requisitos Tecnológicos item 3 "Solução de segurança para Servidores (Linux e Windows), com XDR e Sandbox , com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses"

Deve prover as seguintes proteções:

Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

Deve ser capaz detectar vírus, worms, trojans, toolkits, adware, auto-dialers e outros tipos de ameaças;

Deve possuí módulo de proteção baseado em comportamento;

Deve possuí funcionalidade para inventário de todos os arquivos executáveis de aplicativos;

Deve ser possível a criação de regras especiais para bloquear a instalação e/ou execução de uma aplicação;

Deve ter a capacidade de controlar a aplicação utilizando o caminho, hash, nome da aplicação;

Deve possuir funcionalidade de scan de drives removíveis, tais como: CDs; DVDs; Discos Blu-ray; Flash drives; HDs externos;

Deve fornecer os seguintes controles para dispositivos externos conectados ao

computador:

Por tipo de dispositivo;

Por barramento de conexão.

As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

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;

Gerenciamento de Quarentena: Deve bloquear objetos suspeitos;

Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);

Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

Capacidade de verificar objetos usando heurística;

Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

5.2.1.3 Requisitos Tecnológicos item 4 - Serviços de Instalação, Configuração e Implantação da Solução (parcela única)

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

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

A instalação, atualização ou migração das consoles de gerência da solução será realizada no TRE-PB;

Deverá ser realizada a instalação, atualização ou migração dos softwares em até 10 (dez) estações de trabalho;

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

A instalação, atualização ou migração da solução deverá ser realizada em horário de expediente de cada sítio, podendo ocorrer no período de 8h às 20hs;

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

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

Em caso de migração de solução, a CONTRATADA deverá realizar a migração de todas políticas, regras e customizações configuradas no CONTRATANTE;

A CONTRATADA deverá se reunir com a equipe técnica da CONTRATANTE e

elaborar um plano de migração, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço de migração;

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

A instalação, atualização ou migração dos softwares em servidores de rede e das estações de trabalho não pode interferir no bom funcionamento de outros sistemas previamente instalados.

5.2.2. Requisitos de Capacitação item 5

A CONTRATANTE solicitará cada turma de transferência de conhecimento por e-mail, com um prazo igual ou superior a 15 dias corridos para o início da sua execução.

A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do Contratante, por meio de treinamento oficial nas tecnologias da solução, com carga horária total de, no mínimo, 40 (quarenta) horas. A carga horária diária não poderá ser inferior a 4h (quatro horas) e nem superior a 8h (oito horas).

O treinamento deverá ocorrer em dias úteis e em horário comercial.

A transferência de conhecimento deverá ser realizada de forma remota ou poderá ser realizado nas dependências do Tribunal Superior Eleitoral, conforme decisão do CONTRATANTE.

Cada turma referente a transferência de conhecimentos será compostas de: no mínimo 10 (dez) e no máximo 20 (vinte) alunos.

A transferência de conhecimento deverá conter conteúdo teórico e prático e deverá abordar, no mínimo, os seguintes itens:

Detalhamento dos componentes da solução, suas interconexões e todas as informações técnicas necessárias para o seu pleno funcionamento.

Orientar sobre os componentes, procedimentos de instalação e administração da solução unificada de segurança para endpoint e EDR, explorando todas as funcionalidades exigidas na especificação técnica.

Orientar sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos e virtuais da solução, informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE.

Orientar sobre os componentes, procedimentos de instalação e administração da solução, explorando as funcionalidades disponíveis na solução ofertada, ainda que não exigidas na especificação técnica.

O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a solicitação realizada por e-mail, no prazo de 7 dias corridos.

Caso o CONTRATANTE solicite alterações no programa de transferência de conhecimento, a CONTRATADA terá até 2 (dois) dias corridos para apresentação de uma nova versão do programa. Eventuais mudanças de conteúdo solicitadas pelo CONTRATANTE deverão constar no material didático.

O CONTRATANTE terá até 2 (dois) dias úteis para aprovação da nova versão do programa. Deverá ser disponibilizado material didático em formato digital, sem custo adicional para o CONTRATANTE.

Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).

Deverá ser emitido certificado de participação ao final do curso a cada

participante, detalhando programa e carga horária.

Ao final da transferência de conhecimento, a CONTRATADA deverá aplicar um questionário de avaliação para preenchimento obrigatório de todos os servidores treinados, previamente acordado com a fiscalização do contrato.

Será considerado como satisfatório o percentual de aprovação acima de 70% (setenta por cento).

Caso a transferência de conhecimento não seja satisfatória em relação aos aspectos relacionados à carga horária, programa apresentado e estrutura, esta deverá ser realizada novamente, sem ônus adicional ao CONTRATANTE.

A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelo fabricante dos softwares da solução ofertada.

5.2.3. Requisitos Legais

5.2.3.1 - Margem de Preferência

Não há.

5.2.4. Requisitos de Manutenção

Não há requisitos de manutenção dos itens adquiridos.

5.2.5. Requisitos Temporais

- O suporte e a garantia de atualização do software deve ser de, no mínimo, 60 (sessenta) meses;

5.2.6. Requisitos de Segurança

5.2.6.1. A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação do da Justiça Eleitoral, obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral da Paraíba aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

5.2.6.2. O Tribunal Regional Eleitoral da Paraíba terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

5.2.6.3. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).

5.2.6.4. O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

5.2.7. Requisitos de Instalação

- A Contratada será inteiramente responsável pela instalação e configuração da solução, bem como às despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;
- A instalação da solução deverá ser realizada sem causar indisponibilidade do ambiente;
- O processo de instalação da solução deverá ser acompanhado por servidores da Contratante;

- Para garantir que a instalação não afetará o ambiente da Contratante, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante;
- A Contratada deverá se reunir com a equipe técnica da Contratante e elaborar um plano de instalação, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço;
- A instalação da solução no ambiente da Contratante não poderá interferir no bom funcionamento de outros sistemas previamente instalados

5.2.8. Requisitos Sociais, Ambientais e culturais

5.2.8.1. Logística Reversa

5.2.8.1.1. É de responsabilidade da CONTRATADA a disposição final responsável e ambientalmente adequada das embalagens e materiais que porventura venham a ser utilizados em observância à Logística Reversa disposta no art. 33 da Lei Nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos;

5.2.8.1.2. O Tribunal reserva-se o direito de assumir a responsabilidade a que se refere o item anterior, podendo dar outra destinação às embalagens e materiais após o uso, caso julgue mais conveniente para a Administração;

5.2.8.1.3. Qualquer material que venha a ser utilizado na embalagem dos produtos ofertados e/ou utilizados na execução dos serviços deverão ter sua reciclabilidade efetiva no Brasil.

6. Levantamento das Alternativas Disponíveis no Mercado

As soluções presentes no presente estudo resumem-se as seguintes opções.

6.1. Soluções

6.1.1. SOLUÇÃO 1: Licitar uma Solução de Antivírus sem EDR/XDR

Vantagens: Preço baixo e conhecimento da equipe pois é modelo de antivírus atualmente adotado pelo tribunal.

Desvantagens: Quando se fala em detecção de ameaças desconhecidas e/ou nunca vistas, as soluções tradicionais de endpoint não possuem capacidade de detecção das mesmas, uma vez que não possuem sandbox. As soluções de EDR costumam resolver este tipo de problema.

6.1.2. SOLUÇÃO 2: Licitar uma Solução de Antivírus com EDR/XDR

Vantagens: É uma categoria de ferramentas de segurança que monitoram dispositivos de hardware do usuário final em uma rede para detectar uma variedade de atividades e comportamentos suspeitos, reagir automaticamente ao bloquear ameaças percebidas e salvar dados médicos legistas para uma investigação mais aprofundada. Atualmente a proteção de EDR, aliada a proteção de endpoint, se tornou um requisito mínimo para proteção adequada do ambiente, provendo maior capacidade de detecção e principalmente de resposta a atividades maliciosas em endpoints. Uma solução de EDR atua na camada de proteção a endpoints, minimamente, com:

Detecção de arquivos e ações maliciosas baseado em comportamento;

Detecção de scripts e comandos mal intencionados a partir de playbooks e padrões de execução;

Detecção de ataques do tipo “Live off the Land”; Amplia a camada de

visibilidade quanto ao status de endpoints em relação a atividades maliciosas;

Registro de eventos e qualificação daqueles que de fato precisam ser analisados;

Ampliação da camada investigativa, através de coletas de evidências para análise forense;

Estabelecimento de um framework eficiente para resposta a incidentes de segurança; Execução de arquivos em sandbox para detecção de zero day.

Desvantagens: Preço mais elevado quando comparado com uma solução de antivírus normal (sem EDR) e mais elevado que aderir a ata do TSE (solução 3), Custos de um processo licitatório além da necessidade de contratação dos itens 4 (Instalação e Configuração) e 5 (Repasse Tecnológico) .

Fornecedores que atendem a demanda: Blue Eye (Cotação 1183094), Brasofware (Cotação 1183162) e Itware (Cotação 1183177)

Soluções de Fabricantes que atendem a demanda:

I - Trend Micro Enterprise Security for Endpoints e Trend EDR/XRD for Users

II - Symantec Endpoint Security Complete

III - FireEye Endpoint Security Crowdstrike Falcom Endpoint Protection Premium

6.1.3. SOLUÇÃO 3: Adquirir a Solução de Antivírus com EDR/XDR por meio da adesão a ATA do TSE

Vantagens: Além de todas as vantagens descritas na SOLUÇÃO 2, ao aderir a ata do TSE o TRE-PB irá receber gratuitamente

do TSE os itens 4 (Instalação e Configuração) e 5 (Repasse Tecnológico) conforme explicado no e-mail (1180421). O TRE-PB

estará padronizado com toda a justiça eleitoral no que diz respeito a solução de antivírus e não necessitará arcar com os

custos de um processo licitatório.

Desvantagens: Preço mais elevado quando comparado com uma solução de antivírus normal (sem EDR).

Fornecedores que atendem a demanda: DFTI (ata Nº 1/2022 TSE 1179380),

Solução de Fabricantes que venceu a ata do TSE e atende a demanda:

Trend Micro Enterprise Security for Endpoints e Trend EDR/XRD for Users

6.2. Análise de Custos Totais das Soluções de TIC Identificadas

Os custos estimados da contratação são conforme tabela abaixo baseada nas cotações dos fornecedores e na ata de registro de preços do TSE levando em consideração apenas os item 03 pois os demais itens (1,2,4 e 5) serão fornecidos pelo TSE conforme explicado nos e-mails (1183094) e (1187651) .

Item	Fornecedor	Descrição/Modelo	Quantidade Registrada	Valor Unitário Anual	Valor Unitário (Por 60 meses)	Valor Global (Por 60 meses)
6.1.1.-03	Blue Eye	Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	200	R$ 220,00	R$ 1100,00	R$ 220.000,00
6.1.2-03	Brasoftware	Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	200	R$ 124,65	R$ 623,25	R$ 124.650,00
6.1.2-03	Itware	Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	200	R$ 137,02	R$ 655,10	R$ 131.020,00
6.1.3-03	ATA TSE	Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	200	R$ 46,00	R$ 230,00	R$ 46.000,00

7. Justificativa da Solução Escolhida

De acordo com as soluções levantadas temos as seguintes considerações:

- A solução 1 (Licitar Antivírus sem EDR/XDR) embora seja a menos cara, não atende a todas necessidades de negócio e a todos requisitos tecnológicos necessários para proteger o tribunal das inúmeras ameaças avançadas de malwares. O tribunal também iria ficar não padronizado com relação a solução de antivírus adotado por toda a justiça eleitoral.

- A solução 2 (Licitar Antivírus com EDR/XDR) embora atenda a todas necessidades de negócio e a todos requisitos tecnológicos é a que apresenta o maior preço de todas as soluções, além dos custos envolvidos em um processo licitatório e dos custos envolvidos na aquisição do item 4 (instalação e configuração) e do item 5 (repasse tecnológico). Caso o tribunal optasse pela solução 2 existiria uma grande chance de ficarmos não padronizados com toda a justiça eleitoral com relação a solução de antivírus, se o vencedor da licitação apresentasse uma proposta de fabricante distinto do fabricante apresentado na ata do TSE que será adotada por toda a justiça eleitoral.

- A solução 3 (Adquirir Antivírus com EDR por meio de adesão a ATA do TSE) é a que melhor solução, pois atende, com o menor custo, a todas necessidades de negócio e a todos requisitos tecnológicos além de manter o tribunal padronizado com toda a justiça eleitoral no que diz respeito a solução de antivírus. Com a solução 3 também não será necessário para o tribunal arcar com os custos de um processo licitatório.

7.1. Solução Escolhida

Nome: SOLUÇÃO 3

Descrição: Adquirir Antivírus com EDR/XDR por meio de adesão a ata Nº 1/2022 TSE 1179380 .

Valor Estimado : R$ 46.000,00 (Quarenta e seis mil reais).

7.2. Benefícios Esperados

As credenciais privilegiadas dos principais ativos de TI estarão protegidas, mitigando riscos de ataques cibernéticos e protegendo os sistemas de tecnologia da informação da Justiça Eleitoral e Conformidade com normas de gestão de segurança da informação.

7.3. Alinhamento em relação às necessidades

A solução escolhida se alinha perfeitamente com as necessidades do negócio e com os requisitos tecnológicos.

7.4. Relação entre a demanda prevista e a quantidade dos bens e/ou serviços a serem contratados

Considerando o fato de o tribunal possuir aproximadamente 140 servidores (Linux e Windows) com expectativa de crescimento para 200 servidores nos próximos 5 anos.

Considerando o fato que os itens 1,2,4 e 5 serão fornecidos ao TRE-PB gratuitamente pelo TSE.

Para atender a demanda existente o TRE-PB deverá adquirir:

Lote	Item		Unidade	Quantidade Inicial Estimada	Quantidade Total Registrada	Valor Unitário Médio (por 60 meses)	Valor Total
1	3	Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	Unidade	130	200	R$ 230,00	R$ 46.000,00
1	**VALOR TOTAL DO LOTE**						**R$ 46.000,00**

8. Necessidades de Adequação do Ambiente do Órgão

Não haverá necessidade de adequação do ambiente, tendo em vista que a contratação não alterará em nada o ambiente atualmente em uso.

Seção II - SUSTENTAÇÃO DO CONTRATO

Como não há nenhuma consideração a ser feita no tocante à estratégia de sustentação do contrato, estaremos suprimindo esta parte.

Seção III - ESTRATÉGIA PARA A CONTRATAÇÃO

9. Natureza do objeto

Trata-se de uma subscrição para uso de software, cujo uso é comum a diversas instituições da Administração Pública Federal, sendo assim um padrão de mercado.

10. Parcelamento do objeto

O objeto pode ser dividido pelos itens que compõem a solução.

11. Adjudicação do objeto

A adjudicação do objeto pode ser feito por lote, que podem ser fornecidos por diferentes empresas, tendo em vista que os itens do lote compõem uma solução global, interdependente e indivisível.

12. Modalidade e tipo de licitação

Após realização dos estudos técnicos chegou-se aos seguintes quantitativos de material, descrito no item 7.4, a serem licitados em lote único e através do sistema de Registro de Preços (por se tratar de uma IRP conduzida pelo TSE):

13. Classificação e indicação orçamentária

Recursos suplementares de cibersegurança oriundos de iniciativa do TSE

3.3.90.40.21.0021 - SERVIÇOS TÉCNICOS PROFISSIONAIS DE TIC

14. Vigência da prestação de serviço

A vigência dos itens registrados será de 60 meses.

15. Equipe de Apoio à Contratação

A equipe de apoio à contratação será composta pela mesma equipe do presente estudo preliminar constante do item 02 deste documento.

16. Equipe de Gestão da Contratação

Sugerimos como gestor titular do contrato o servidor Felipe Cavalcanti Alves e o substituto o servidor Airton Alves de Medeiros Júnior.

Seção IV - ANÁLISE DE RISCOS

17. Riscos do Processo de Contratação

Os riscos do processo da contratação e as respostas aos mesmos estão descritos na planilha 1185548.

FELIPE CAVALCANTI ALVES
RESPONSÁVEL PELO NÚCLEO DE SEGURANÇA DA INFORMAÇÃO

Documento assinado eletronicamente por FELIPE CAVALCANTI ALVES em 15/02/2022, às 11:46, conforme art. 1º, III, "b", da Lei 11.419/2006.

AIRTON ALVES DE MEDEIROS JUNIOR
TÉCNICO JUDICIÁRIO

Documento assinado eletronicamente por Airton Alves de Medeiros Junior em 15/02/2022, às 11:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

SORAYA BEZERRA CAVALCANTI NORAT
ANALISTA JUDICIÁRIO

Documento assinado eletronicamente por SORAYA BEZERRA CAVALCANTI NORAT em 15/02/2022, às 12:48, conforme art. 1º, III, "b", da Lei 11.419/2006.

PEDRO DE FIGUEIRÊDO LIMA NETO
CHEFE DA SEÇÃO DE INFRAESTRUTURA DE REDE

Documento assinado eletronicamente por PEDRO DE FIGUEIRÊDO LIMA NETO em 15/02/2022, às 15:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pb.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1188597&crc=78F493D4, informando, caso não preenchido, o código verificador **1188597** e o código CRC **78F493D4**..