TRIBUNAL SUPERIOR ELEITORAL

ESTUDOS TÉCNICOS PRELIMINARES

I – Apresente a necessidade a ser atendida:

Garantir proteção contra vírus de computador e ameaças conhecidas, seja nos desktops físicos e virtuais, quanto nos servidore

II – Indique o público-alvo (unidades orgânicas, autoridades, servidores, outros) da contratação:

Todos os usuários que fazem uso do ambiente computacional da rede da Justiça Eleitoral.

III – Indique a(s) consequência(s), caso não haja atendimento da necessidade:

O não atendimento da necessidade trará para a rede da Justiça Eleitoral risco de infecções causadas por códigos maliciosos (r
ações danosas e atividades maliciosas em um computador.

Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- Pela exploração de vulnerabilidades existentes nos programas instalados;
- Pela auto execução de mídias removíveis infectadas, como pendrives;
- Pelo acesso às páginas Web maliciosas, utilizando navegadores vulneráveis;
- Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas;
- Através de mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recur

Uma vez instalados, os malwares passam a ter acesso aos dados armazenados no computador e podem executar ações malicios

Seguem abaixo exemplos na imprensa de casos de ataques a órgãos públicos:

STJ

https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04122020-STJ-Noticias-destaca-reforco-na-seguranca-de-

TJ-RS

https://www.correiodopovo.com.br/not%C3%ADcias/geral/tj-rs-confirma-ataque-cibern%C3%A9tico-que-tirou-sistemas-do-a
8IQ9XDXYf32Qf0KRthgjPjZEdBZ0T2jf9qE53byQTFOaI

https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04122020-STJ-Noticias-destaca-reforco-na-seguranca-de-

IV – Indique o alinhamento da necessidade ao Planejamento Estratégico do TSE:

A presente contratação encontra-se alinhada ao Plano Estratégico do TSE 2018/2021, aprovado por meio da Resolução nº 23. Plano Geral de Contratações (PGC) 2020-2021, que se encontra em tramitação neste Tribunal.

- Integração: compartilhamento de experiências, conhecimentos e colaboração participativa na Justiça Eleitoral que conduzam à for
- Celeridade: atuação com rapidez e agilidade, garantindo a qualidade do resultado entregue;
- Confiabilidade: atuação com eficiência e eficácia, de acordo com as atribuições normativas;
- Inovação: estímulo à criatividade e à busca de soluções diferenciadas;

Além desses Valores, mostram-se alinhados com a presente contratação os seguintes Objetivos:

- Objetivo 1 Assegurar a legitimidade do processo eleitoral;
- Objetivo 3 Fomentar a aproximação da Justiça Eleitoral com a sociedade;
- Objetivo 4 Aprimorar os mecanismos de transparência;
- Objetivo 5 Aprimorar a gestão da informação e do conhecimento;
- Objetivo 6 Aprimorar a gestão de processos organizacionais
- Objetivo 8 Aperfeiçoar a governança institucional;
- Objetivo 11 Garantir a eficiência na prestação dos serviços de tecnologia da informação e comunicação.

A contratação decorrente deste processo está, também, alinhada aos objetivos do Planejamento Estratégico de Tecnologia da dispõe sobre a estratégia de TIC do Tribunal para o período de 2018 a 2021.

- Objetivo 1: Ampliar a segurança do processo eleitoral por meio de serviços e soluções de TI;
- Objetivo 2: Ampliar a transparência dos serviços e das soluções de TI que suportam o processo eleitoral informatizado;
- Objetivo 3: Modernizar os serviços e as soluções de TI que suportam o processo eleitoral.
- Objetivo 4: Prover e ampliar os serviços e as soluções de TI que suportam as áreas administrativas e judiciais do TSE;
- Objetivo 5: Ampliar a prestação dos serviços e das soluções de TI que suportam a entrega dos serviços públicos providos pelo Tri
- Objetivo 6: Primar pela satisfação dos clientes de serviços e soluções de TI;
- Objetivo 7: Aprimorar as práticas e os controles de segurança da informação utilizados no desenvolvimento e na operação de ser
- Objetivo 8: Garantir a infraestrutura e os recursos tecnológicos adequados às atividades estratégicas do TSE;
- Objetivo 10: Aprimorar as práticas de governança de tecnologia da informação.

V – Indique o resultado da pesquisa de mercado para identificação das soluções que possam atender às necessidades explicita

Atualmente, temos instalada uma solução que apenas contempla a função de antivírus no parque computacional da Justiça noticiadas diariamente na mídia, sobretudo em órgãos públicos e grande empresas, esta solução não atende mais às necessidades da Ju

Busca-se nesta aquisição incluir, além da função de antivírus, a inclusão da funcionalidade de EDR (Endpoint Detection and cibernética projetadas para detectar e remover qualquer malware ou qualquer outra forma de atividade maliciosa em uma rede.

O EDR vai além do antivírus, detecta e reage a atividades suspeitas e fornece dados forenses aos analistas de segurança.

Trata-se, portanto, de uma categoria de ferramentas de segurança que monitoram dispositivos de hardware do usuário fina suspeitos, reagir automaticamente ao bloquear ameaças percebidas e salvar dados para uma investigação mais aprofundada.

Sendo assim, para elaboração deste Estudo Preliminar foram levadas em consideração duas possibilidades, sendo:

- **Solução 1º: Solução de Antivírus**
- **Solução 2º Solução de Antivírus + EDR**

Opções de mercado	Detalha
1ª) Antivírus	Uma solução antivírus oferece proteção constante para todos c de rede que possam estar sujeitos a ataque por vírus ou outro r **Vantagens:** Preço baixo e conhecimento da equipe. **Desvantagens:** Quando se fala em detecção de ameaças descc possuem capacidade de detecção das mesmas, uma vez que nã problema. **Preço Estimado:** R$ 1.983.691,20 (um milhão, novecentos e
2ª) Antivírus + EDR (detecção e resposta do endpoint).	**Vantagens:** É uma categoria de ferramentas de segurança que detectar uma variedade de atividades e comportamentos suspe médicos legistas para uma investigação mais aprofundada. Atu requisito mínimo para proteção adequada do ambiente, proven maliciosas em endpoints. Uma solução de EDR atua na camad • Detecção de arquivos e ações maliciosas baseado em co • Detecção de scripts e comandos mal intencionados a pa • Detecção de ataques do tipo "Live off the Land"; • Amplia a camada de visibilidade quanto ao status de en • Registro de eventos e qualificação daqueles que de fato • Ampliação da camada investigativa, através de coletas c • Estabelecimento de um framework eficiente para respos • Execução de arquivos em sandbox para detecção de zer **Desvantagens:** Preço mais elevado quando comparado com u Órgãos públicos que adotaram essa solução: Exército Brasilei Agricultura, Ministério do Meio Ambiente, Secretaria de Segu **Preço estimado**: R$ 3.188.925,00 (três milhões, cento e oiten

Observação: Em ambos os casos deverão ser levados em consideração ainda os custos do serviço de instalação e da transferê ano.

- Item 4: Serviços de instalação, configuração e implantação da solução (parcela única), em 28 sítios da rede da Justiça Eleitoral, send
- Item 5: Transferência de conhecimento (parcela única): R$ 89.000,00

Estimativa do Valor Total dos Serviços (apenas no 1º ano): R$ 387.611,60.

Segue abaixo lista de alguns fabricantes que atendem a necessidade do TSE:

Solução Identificada	Deta

Soluções	a) **Trend Micro Enterprise Security for Endpoints e Trend EDR/XRD for Users**	Fornece um conjunto abrangente de técnic atuais ameaças em constante evolução. Essa suíte proteção contra ameaças e segurança de dados pa qualquer dispositivo e aplicativo. É possível gerenciar a atividade do usu implementação a partir de uma só console, dand ambiente. Proteção completa de desktops e dispositivo sofisticadas. • Consolida os endpoints abaixo de uma infraes • Proteção real-time para servidores de arquiv disseminação de vírus, spywares e outras ame • Gerenciamento centralizado de ameaças e da TI, simplificando o gerenciamento e provendo **Trend EDR/XRD for users - *Recursos de detecção*** As organizações enfrentam um massacre contornar as medidas de segurança existentes. avançada, é essencial para eliminar ou minimizar o i A detecção e resposta do endpoint (EDR endpoint, investigar a causa raiz e mitigar o impacto influenciar partes importantes do caminho de ata entrou na organização por e-mail, não pode oferec portanto, não pode remover ou impedir a propaga mails, a combinação de e-mail com detecção e respo **PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS** • O Apex One utiliza uma combinação de técnic todos os tipos de ameaças. Oferece segurança eficácia. • O Cloud App Security fornece proteção avanç nuvem. É uma solução integrada de API que mail de terceiros para adicionar detecção comprometimento de e-mail comercial (BE (Microsoft® OneDrive® for Business, Microsc • Uma proteção forte e integrada de ameaças e defesas, resultando em menos eventos para in • O uso da integração entre soluções de endpo priorização de ameaças em comparação com **PRINCIPAIS RECURSOS DE PROTEÇÃO** • Aprendizado de máquina de alta fidelidade (p • Análise comportamental (contra scripts, injeçã • Web reputation; • Prevenção de exploração (firewall do host, pr • Bloqueio de Command and Control (C&C); • Proteção de Vulnerabilidades; • Controle de Aplicações; • Controle de dispositivos; • Integração com sandbox e detecção de violaçã • Criptografia de Endpoint (requer agente sepa

b) **Symantec Endpoint Security Complete**	O aumento dos ataques direcionados e ata proteção em camadas e segurança inteligente no excelente desempenho e gerenciamento inteliger informações civis sobre ameaças do mundo, a Syma dia zero sem prejudicar seu desempenho. O Syma com um único agente de alta potência para proporc Principais recursos: • Alta Segurança : bloqueia ataques direciona endpoint; • A proteção contra ameaças à rede analisa os f • Utiliza a maior rede de inteligência global d sensores que alimentam de dados as nossas te • A análise de reputação da tecnologia Insight detecção mais rápida e precisa; • A análise comportamental da tecnologia SONA ataques direcionados e ameaças de dia zero; • Proteção de antivírus, antispyware e firewall r • Excelente desempenho: otimizado para fornec • A tecnologia Insight exige somente a verifi verificação; • Tamanho do cliente reduzido com menor espa • Carga de rede reduzida com flexibilidade para • Gerenciamento inteligente: console de gerenc de políticas; • Agente único de alto desempenho com um ú virtuais e sistemas incorporados; • Suporte para implementação remota e gerenc • Controle granular de políticas com bloqueio d

	c) **FireEye Endpoint Security**	**FireEye Endpoint Security** - *Envolve vários mecanis* A segurança tradicional de estações não é ataques sofisticados ou avançados de ameaças per solução deve analisar e responder rapidamente a es O FireEye Endpoint Security combina o tecnologia FireEye, conhecimento e inteligência pa mecanismos no Endpoint Security para impedir, det Para evitar o malware comum, o Endpoint (EPP) com base em assinatura. Para encontrar am usa o machine learning alimentado de conhecimento avançadas, os recursos de detecção e resposta do de análise baseado em comportamento. Por fim, um que se baseia na inteligência atual da linha de f profunda ajuda a proteger as informações vitais arn Mesmo com a melhor proteção, as violaçõe a interrupção dos negócios, o Endpoint Security for • Pesquisar e investigar ameaças conhecidas simultaneamente; • Identificar e detalhar vetores de ataque usado • Determinar se um ataque ocorreu (e persiste) • Estabelecer uma linha do tempo de incidente ameaça; • Identificar claramente quais terminais e sistem Principais recursos: • Impedir a maioria dos ataques cibernéticos co • Detectar e bloquear violações que ocorrem pa • Melhorar a produtividade e a eficiência descol • Usar um único agente de tamanho reduzido pa • Compliance com regulamentos, como PCI-DSS • Possuir várias opções de deployment.
	d) Crowdstrike Falcom Endpoint Protection Premium	O Falcon Endpoint Protection Premium da reúne um antivírus de última geração (NGAV), detec inteligência integrada de ameaças e higiene de TI. Além de impedir ataques, o Falcon Endpoin • Preparar-se antes de ocorrer um ataque acre isso identifica sistemas desprotegidos e descor usadas no ambiente; • Confirma sua preparação com verificaçõ recomendações de segurança dos especialista • Incluir todos os componentes necessários par • Implementar em minutos e operacionalização • Praticamente zero de impacto nos endpoints; • Atualizar facilmente a partir de uma solução CrowdStrike Falcon sem a necessidade de nov • Atualização automática com entrega de softwa • Adaptação a qualquer necessidade, crescimen

Figura 1 - Plataformas de Proteção de Endpoints (Gartner 2021)

Neste quadrante, entende-se como Líder (*Leaders*) o conjunto de empresas que demonstrou esforço e um progresso equilibrad

As Desafiadoras (*Challengers*) são aquelas empresas que possuem produtos antimalware sólidos que abordam as necessidades

As visionárias (*Visionaries*) são aquelas que investem em recursos inovadores como o malware avançado e recursos de prote com possibilidade de ofertar aos compradores acesso antecipado a uma melhor segurança e gerenciamento.

Por fim, as empresas de nicho de mercado (*Niche Player)* oferecem soluções sólidas de antimalware, mas raramente lideram o r

Diante desta breve análise do mercado de soluções de proteção de segurança, constata-se que o mercado é diversificado.

Além disso, depreende-se dessa análise de mercado que as funcionalidades apresentadas por essas soluções são comuns a di oferta de diferentes soluções com resultados e benefícios similares.

O modelo de negócio adotado pelo mercado de antivírus consiste na venda de licenciamento perpétuo ou subscrição do produ

Ambos com direito a atualização do software por período pré-definido, além da prestação de serviços correlatos, tais como sup

Justificativa de escolha das soluções:

Todas as soluções acima estão sendo consideradas neste estudo pelos seguintes fatores:

- Possuem itens que vão de acordo com as necessidades especificadas;
- As soluções já participaram de diversos projetos similares em outras organizações governamentais;
- Possuem bom desempenho em relatórios recentes de plataformas reconhecidas de medição de qualidade de software;
- São bem avaliadas em fóruns e páginas que discutem segurança da informação na internet.

Análise técnica comparativa

As soluções listadas acima dão uma visão de como o mercado atende as necessidades atuais e também a mostra a ampla e especificações técnicas ainda serão elaboradas a nível micro durante a elaboração do Termo de Referência.

Resumo de pregões públicos semelhantes

Foram utilizados como referência apenas pregões cujo o contrato ainda consta como ativo.

Pregão 1 – Tribunal Regional do Trabalho - 13ª Região

Pregão eletrônico 11/2021

Descrição: Registro de Preços objetivando a eventual aquisição de solução de Segurança de Endpoints, com garantia de atualiz

Data da abertura das propostas: 22/06/2021

Valor total estimado: R$ 25.663.221,89

Solução Identificada: Antivírus + EDR

Pregão 2 – Defensoria Pública do Pará

Pregão eletrônico 03/2021

Descrição: Contratação de empresa para fornecimento de subscrição de softwares de segurança, incluindo garantia, atualiza serviços técnicos especializados, conforme especificações e quantidades previstas no termo de referência, para atender as necessidade

Data: 02/02/2021

Valor total : R$ 8.112.930,00

Solução Identificada: Antivírus + EDR

Pregão 3 – SEDUC – RO

Pregão Eletrônico n° 290/2019

Descrição: Registro de preço de aquisição de equipamentos e materiais permanentes e serviços – solução unificada de segu avançados, com garantia de 36 meses, contemplando pacote de instalação e configuração, treinamento (hands-on) e operação assistida

Data: 08/10/2019

Valor total : R$ 9.023.454,00

Solução Identificada: Antivírus + EDR

Pregão 4 – Defensoria Pública da União

Pregão Eletrônico n° 1/2018

Descrição: Contratação de Soluções de Segurança integradas: Fornecimento de licença de uso, sua respectiva manuten Gerenciamento Seguro da Informação e Solução integrada Segurança Digital com conceito de blindagem do domínio web, incluind aquisição e manutenção, baseado nas soluções de mercado conforme Edital e Termo de Referência seus anexos.

Data: 17/01/2018

Valor total : R$ 7.907.240,00

Solução Identificada: Antivírus + EDR

Pregão 5 – ANVISA

Pregão Eletrônico n° 6/2017

Descrição: Aquisição e renovação de licenças para expansão de solução de Segurança da plataforma de produtos SYMANTEC trabalho (desktops), servidores de rede e das informações, com garantia de funcionamento "on-site" pelo período de 12 (doze) meses, serviços de implantação, garantia de atualização contínua, suporte técnico "on-site" e repasse de conhecimento de toda a solução.

Data: 07/04/2017

Valor total : R$ 13.571.801,00

Solução Identificada: Antivírus + EDR

Pregão 6 – Ministério do Meio Ambiente

Pregão Eletrônico n° 6/2018

Descrição: Registro de preços para atualização e suporte referente às licenças da solução de Segurança da plataforma de pro prover segurança e proteção para estações de trabalho (desktops), servidores de rede e das informações institucionais, objetivando a conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Data: 28/11/2018

Valor total : R$ 6.277.060,40

Solução Identificada: Antivírus + EDR

PESQUISA DE PREÇO DE SOLUÇÃO:

Lote	Item	Descrição	Quantidade
1	**1**	Solução de segurança de EndPoint (**desktops dos ambientes dos 27 TREs**), com **EDR e Sandbox** , com manutenção, garantia (update e upgrade) e suporte por 60 meses, com pagamento de subscrições a cada 12 meses.	32.000
	2	Solução de Segurança de EndPoint (**desktops do ambiente do TSE**), com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) e suporte por 60 meses, com pagamento de subscrições a cada 12 meses.	2.500
	3	Solução de Segurança para Servidores (**Linux e Windows para ambientes do TSE e 27 TREs**), com XDR e Sandbox, com manutenção, garantia (update e upgrade) e suporte por 60 meses, com pagamento de subscrições a cada 12 meses.	5.000
	3	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única).	28
	4	Transferência de conhecimento (parcela única).	4 turmas

VI – Indique a descrição completa da solução que, por entendimento do(s) signatário(s) deste documento, melhor atenderá à necessidade

A solução n.º 2 (Antivírus + EDR) é a que melhor atende a necessidade porque, devido a evolução das ameaças atuais, bem cor
a única que seria eficiente na proteção do parque computacional da Justiça Eleitoral.

IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

- Proteção avançada antimalware para estações de trabalho e servidores de rede.
- Proteção contra execução de aplicações maliciosas.
- Análise e bloqueio da execução de aplicações baseada em comportamento.
- Monitoramento de atividades de criptografia de arquivos para evitar ataques de ransomware.
- Proteção contra ataques direcionados e 0Day.
- Proteção para a solução de correio eletrônico do TSE com capacidade de atendimento ao tráfego de e-mail gerado.

DESCRIÇÃO RESUMIDA DA SOLUÇÃO:

- Aquisição de soluções de seguranças do tipo Solução de Antivírus, incluindo licenciamento, serviços de instalação, suporte técnicc
- 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
- A solução deve se auto proteger contra ataques aos seus serviços e processos e deve ter a capacidade de implementar a funciona
- A solução deve contemplar proteção contra ataques: direcionados e suas variantes, 0Day (dia zero), vulnerabilidades desconhecic 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 vulnerabilidades.
- A solução deve ter a capacidade de receber instruções de comando contra ataques de APT (Ameaça Persistente Avançada) ou sim 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 r
- Capacidade de limitar o acesso dos sistemas e aplicativos a recursos do sistema operacional, como chaves do registro e pastas e a
- 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
- Implementar a proteção contra acesso a websites ou URLs consideradas maliciosas, de baixa reputação ou não categorizadas.

A solução escolhida é composta por 5 itens, sendo eles:

Item 1: Solução de Segurança de Endpoint (desktops dos ambientes dos 27 TRE), com EDR e Sandbox, com manutenção, garan

- Proteção avançada antimalware para estações de trabalho dos 27 TRE.
- 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 varian 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 có
- Detecção e remoção de vírus de macro.
- Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que 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.

Item 2: Solução de Segurança de Endpoint (desktops do ambiente do TSE), com XDR e Sandbox, com manutenção, garantia (up

- A solução e suas funcionalidades deverão funcionar com agente único a ser instalado em servidores físicos e virtuais, a fim de din
- 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 versões (32 e 64 bits).
- Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidad
- Proteger de forma automática e transparente contra brechas de segurança descobertas interrompendo somente o tráfego malicio
- Possuir a capacidade de detectar e bloquear ataques em aplicações web tais como: SQL Injection e Cross-Site Scripting dentre out
- O software de proteção deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", assim como, implemer 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 vuln 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 interva
- 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 saída 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 a
- Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do S.O. e demais aplicações, recomendando ações
- 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 g
- Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, os seguintes sistemas operacior
  - 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);
  - Aplicações como: Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Postgree, MySQL Server e suas variantes, A
  - Mozilla Firefox, Microsoft Internet Explorer, Edge, Google Chrome, Safari, Web Server Apache, Tomcat, NGinx, Joomla, Plone,
  - 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
- Permitir que as regras de IPS atuem detectando ou bloqueando os eventos que as violem, de modo que o administrador possa de
- 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*.

Item 3: Solução de Segurança para Servidores (Linux e Windows para ambientes do TSE e 27 TRE), com XDR e Sandbox, com m

- Deve prover as seguintes proteções:
- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou
- 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
- 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 desinfec 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
- Capacidade de verificar objetos usando heurística;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

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 atividades pela sua equipe técnica;
- A instalação, atualização ou migração dos softwares em estações de trabalho poderá ser realizada remotamente, sem causar indis pela CONTRATANTE;
- A instalação, atualização ou migração das consoles de gerência da solução será realizada em 28 (vinte e oito) sítios distintos, conf
- 01 (uma) no Tribunal Superior Eleitoral e 27 (vinte e sete) localizadas nos Tribunais Regionais Eleitorais, sendo uma instalação er
- Deverá ser realizada a instalação, atualização ou migração dos softwares em até 10 (dez) estações de trabalho de cada sítio, ou se
- A instalação, atualização ou migração dos softwares em servidores de rede poderá ser realizada remotamente, devendo ser realiz
- A instalação, atualização ou migração da solução deverá ser realizada em horário de expediente de cada sítio, podendo ocorrer n
- 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
- Em caso de migração de solução, a CONTRATADA deverá realizar a migração de todas políticas, regras e customizações configurac
- A CONTRATADA deverá se reunir com a equipe técnica da CONTRATANTE e elaborar um plano de migração, contendo as etapas, r 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 r
- A instalação, atualização ou migração dos softwares em servidores de rede e das estações de trabalho não pode interferir no bon

Item 5 - Transferência de conhecimento.

- A CONTRATANTE solicitará cada turma de transferência de conhecimento por e-mail, com um prazo igual ou superior a 15 dias cc
- A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do Contratante, por meio de treinamento (quarenta) horas.
- A carga horária diária não poderá ser inferior a 4h (quatro horas) e nem superior a 8h (oito horas). O treinamento deverá ocorre
- A transferência de conhecimento deverá ser realizada de forma remota ou poderá ser realizado nas dependências do Tribunal Su
- 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 pler
  - Orientar sobre os componentes, procedimentos de instalação e administração da solução unificada de segurança para endp técnica.
  - Orientar sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos e virtuais da sol CONTRATANTE.
  - Orientar sobre os componentes, procedimentos de instalação e administração da solução, explorando as funcionalidades di
- O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a solicitação reali
- Caso o CONTRATANTE solicite alterações no programa de transferência de conhecimento, a CONTRATADA terá até 2 (dois) dias cc mudanças de conteúdo solicitadas pelo CONTRATANTE deverão constar no material didático. O CONTRATANTE terá até 2 (dois) di

- Deverá ser disponibilizado material didático em formato digital, sem custo adicional para o CONTRATANTE. Todo material deverá 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 obri 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 apre CONTRATANTE.
- A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelo fabricante dos softwares da so

VII – Indique o(s) estudo(s) realizado(s) ou o(s) critério(s) adotado(s) para definir o cálculo e a quantidade da necessidade:

Quanto ao Item 1 :

No objeto do Contrato TSE nº 106/2016 consta o quantitativo de **31.682** licenças de uso de antivírus, conforme tabela abaixo. I

Este quantitativo estava relacionado com o total de microcomputadores, notebooks e equipamentos servidores da plataforma estão instalados e distribuídos geograficamente no TSE, TREs, Zonas Eleitorais e Centrais de Atendimento, conforme tabela abaixo:

	Antivírus Trend Soma de máquinas TSE+TRE +ZE+CA
AC	225
AL	396
AM	555
AP	289
BA	1231
CE	735
DF	612
ES	430
GO	1021
MA	1241
MG	3141
MS	619
MT	722
PA	935
PB	606
PE	1490
PI	710
PR	2705
RJ	2099
RN	895
RO	329
RR	179
RS	1652
SC	1318
SE	395
SP	4581
TO	671
TSE	1900
Total	31.682

Cabe ressaltar que ao longo deste período não houve outra aquisição de licenças de antivírus. Sendo assim, considerando-se:

- que os números descritos na tabela mostram o retrato da necessidade no ano de 2015;
- que houve um crescimento no quantitativo de microcomputadores nos Tribunais Regionais Eleitorais;
- que o objeto desta contratação trata da aquisição de uma solução para os próximo 5 anos;
- o crescimento computacional no Tribunal Superior Eleitoral ao longo dos cinco anos passados desde a última contratação de solu
- a possibilidade de realização de novas aquisições de microcomputadores por parte do TSE e/ou TREs.

Quanto ao Item 2 : Este item é destinado à instalação nos microcomputadores localizados no ambiente do TSE. Atualmente, pc

Quanto ao Item 3 : É destinado à instalação nos servidores físicos e virtuais localizados no Datacenter do TSE, assim como em

- Atualmente temos instalados no TSE o quantitativo de 1429 servidores virtuais.
- Com relação ao quantitativo de servidores dos TRE, estimamos algo em torno de 110 servidores por regional.
- Logo, se multiplicarmos 110 x 27 chegamos a um total estimado de 2.970 servidores virtuais nos TRE.
- Por fim, somando-se TSE + TRE (1.429 + 2.970) chegamos a um total estimado de 4.399 servidores. Este número é muito dinâm os próximos 5 (cinco) anos no quantitativo de servidores.

Quanto ao Item 4: O serviço de instalação tem como objetivo prover a instalação, atualização ou migração das consoles de g abaixo:

- 01 (uma) no Tribunal Superior Eleitoral e 27 (vinte e sete) localizadas nos Tribunais Regionais Eleitorais, sendo uma instalação er
- Deverá ser realizada a instalação, atualização ou migração dos softwares em até 10 (dez) estações de trabalho de cada sítio, ou se
- Logo, o quantitativo de 28 solicitado tem como objetivo atender a implantação da solução em todos os sítios que compõem a rede

Quanto ao Item 5: A Transferência de conhecimento é destinada para os técnicos da Coordenadoria de Infraestrutura d responsáveis pela administração da solução.

- Para o TSE estimamos o quantitativo de 10 servidores;
- Considerando 2 técnicos por TRE, teremos um público estimado de 54 servidores dos Tribunais Regionais;
- O quantitativo total estimado é de 64 servidores (TSE + TRE).

Portanto, sugerimos que seja realizado um Registro de Preços, conforme quantitativos elencados na tabela abaixo:

Lote	Item	Descrição
1	**1**	Solução de segurança de EndPoint (**desktops dos ambientes dos 27 TREs**), com **EDR e Sandbox** , co suporte por 60 meses, com pagamento de subscrições a cada 12 meses.
	2	Solução de Segurança de EndPoint (**desktops do ambiente do TSE**), com **XDR e Sandbox**, com manuten 60 meses, com pagamento de subscrições a cada 12 meses.
	3	Solução de Segurança para Servidores (**Linux e Windows para ambientes do TSE e 27 TREs**), com **XDR** e upgrade) e suporte por 60 meses, com pagamento de subscrições a cada 12 meses.
	4	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parce
	5	Transferência de conhecimento (parcela única).

CRONOGRAMA DE EXECUÇÃO

A CONTRATADA deverá cumprir os eventos descritos nas tabelas a seguir, respeitando os prazos máximos estabelecidos, os qu

MARCO (dias corridos)	EVENTO	RESPONSÁVEL	
D	Assinatura do contrato	TSE e CONTRATADA	
D+5	Reunião de Planejamento	TSE e CONTRATADA	
D+35	Concluir instalação e configuração da solução nos 28 sítios	CONTRATADA	S
D+45	Recebimento Provisório	TSE	
D+50	Recebimento Definitivo	TSE	Verificação do funcio

Caso a empresa verifique a impossibilidade de cumprir com o prazo de entrega estabelecido deverá encaminhar ao Tribunal so

- Motivo para não cumprimento do prazo, devidamente comprovado, e o novo prazo previsto para entrega.
- A comprovação de que trata esta cláusula deverá ser promovida não apenas pela alegação da empresa CONTRATADA, mas descumprimento de prazo, tais como: carta do fabricante/fornecedor, laudo técnico de terceiros, Boletim de Ocorrência de

VIII – Indique se a solução eleita é divisível ou não, levando em consideração o mercado que a fornece:

A solução deverá funcionar integrada e como um todo, haja vista que são partes integrantes da solução. Sendo assim, há a ne empresa.

Desta forma, a solução é indivisível.

IX – Indique, entre outras, as restrições internas de caráter técnico, operacional, regulamentar, financeiro e orçamentário, que possam difi

Não há restrição de caráter técnico e operacional para a implementação e uso da solução nas instalações da Justiça Eleitoral. Ta
solução similar a que deverá ser contratada.

Identificamos a necessidade de apresentação de atestado de capacidade técnica por parte da empresa a ser contratada, compr

Acerca dos critérios de sustentabilidade, o documento da SEGESA que balizou a definição foi o SEI 1388575.

- A contratada não deve possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às d
- A contratada, ou seus dirigentes, não deve ter sido condenada por infringir as leis de combate à discriminação de raça ou de gênero, a
- Priorização de apresentação de documentos em formato eletrônico.

Optou-se por retirar o PCMSO, visto que não faz sentido avaliar risco ocupacional para este tipo de contratação, haja vista que
software. O objeto em questão trata-se de aquisição de solução de antivírus com entrega imediata.

Necessidades de Adequação do Ambiente para Execução Contratual:

Não há necessidade de adequação do ambiente da Justiça Eleitoral para a implementação da solução a ser contratada, haja
servidor.

Análise de Riscos:

O objetivo deste documento é proporcionar um artefato que possa prever o acontecimento de eventuais riscos, que podem afe
desenvolvidas. Este documento abordará uma estratégia para identificar se o risco está ocorrendo, e possui estratégia para minimiza
ocorrer.

RISCO 1

Descrição do risco:	Solução não oferecer proteção eficiente contra ataques avançados.
Probabilidade:	Baixa
Dano Potencial:	Ocorrência de infecção por vírus e demais malwares, e ineficiência ao mitigá-la colocando em risco a rede d
Ação Preventiva e Responsável:	Acompanhamento constante na atualização da solução, além de visitas técnicas do suporte da contratada. Responsável: STI.
Ação de Contingência e Responsável:	Acionamento dos canais de suporte da contratada. Responsável: STI.

RISCO 2

Descrição do risco:	Contratação frustrada.
Probabilidade:	Média
Dano Potencial:	Necessidade de utilização de computadores com antivírus desatualizados, podendo causar infecções e/ou e
Ação Preventiva e Responsável:	Solicitação de patrocínio para apoiar a realização da contratação. Responsável: STI
Ação de Contingência e Responsável:	Aceitação do risco e notificação aos usuários da Justiça Eleitoral quanto à necessidade de uso de equipamen Orientar aos usuários para que não utilizem dispositivos externos. Responsável: COINF/TSE

RISCO 3

Descrição do risco:	Atraso no fornecimento das licenças.
Probabilidade:	Baixa
Dano Potencial:	Necessidade utilização de computadores com antivírus desatualizados, podendo causar infecções e/ou epid
Ação Preventiva e Responsável:	Acompanhamento da execução do contrato. Realização de reuniões de acompanhamento com a contratada. Responsável: Fiscais do contrato.
Ação de Contingência e Responsável:	Interceder junto à contratada a fim de priorizar a entrega das licenças. Responsável: Fiscais do contrato.

RISCO 4

Descrição do risco:	Empresa contratada não entregar as licenças do antivírus
Probabilidade:	Baixa
Dano Potencial:	Necessidade de utilização de computadores com antivírus desatualizado, podendo gerar infecção por vírus
Ação Preventiva e Responsável:	Acompanhamento rígido da execução do contrato /Responsável: Fiscal do contrato.
Ação de Contingência e Responsável:	Realização de nova contratação. Responsável: STI e SAD.

X – Indique o valor estimado para a contratação:

O valor estimado para essa contratação é de R$ 16.332.236,60 (dezesseis milhões, trezentos e trinta e dois mil duzentos e trint

De toda forma, e no momento oportuno, uma nova cotação de preços será encaminhada pela unidade responsável.

XI – Aquisição anterior no TSE:

Processo nº:	2016.00.000008956-0
Fornecedor:	DFTI - Comércio e Serviços de Informática LTDA
Resultado da análise:	1 - Não houve qualquer problema relacionado a esta contratação. A empresa prestou todos os serviços de ins 2 - Diferença entre o objeto do contrato tse nº 106/2016 versus nova contratação: Atualmente temos instalada uma solução que apenas contempla a função de antivírus no parque computacio antivírus juntamente com a aquisição da funcionalidade de EDR (Endpoint Detection and Response). O EDR é definid detectar e remover qualquer malware ou qualquer outra forma de atividade maliciosa em uma rede. O EDR vai além c analistas de segurança. Trata-se, portanto, de uma categoria de ferramentas de segurança que monitoram dispositiv atividades e comportamentos suspeitos, reagir automaticamente ao bloquear ameaças percebidas e salvar dados médi Hoje, a alta complexidade e sofisticação dos ciberataques demandam muito mais do que as soluções mais básí os antivírus tradicionais não são suficientes para garantir proteção avançada ao ambiente de TI. A partir daí, o **EDR** para negócios e clientes. Com isso em mente, as plataformas de EDR (detecção e resposta em endpoints, na tradução) protegem o identificando comportamentos maliciosos. **Funcionalidades do EDR** • Detecção de ameaças avançadas no ambiente cibernético; • Correção de falhas antes que o erro aconteça; • Monitoramento contínuo de endpoints, quer estejam online ou offline; • Armazenamento de eventos e incidentes de malwares no endpoint; • Capacidade de resposta em tempo real; • Unificação das informações dos endpoints; • Maior visibilidade do ambiente de TI; • Integração com outras soluções de segurança; • Uso de *whitelists* e *blacklists*. Através do monitoramento contínuo e em tempo real, o gerenciamento dos endpoints se torna mais adaptável, **EDR: importância e vantagens** Pode-se dizer que as soluções de EDR oferecem uma segurança coerente com a complexidade do atual cenário Entre as principais vantagens do EDR, podemos citar: • ampla visualização dos ambientes de TI, uma vez que o recurso permite gerenciar as estações de trabalho s • geração de alertas e relatórios; • suporte de diversos sistemas operacionais; • detecção avançada, com a identificação de ameaças altamente sofisticadas; • resposta avançada, incluindo automação de resposta aos ataques e análise; • recursos anti-phishing e anti-malware; • integração com outras soluções de segurança, assegurando um controle mais eficaz das ferramentas de pro Portanto, a tecnologia EDR é a principal diferença entre o objeto desta contração e o objeto do contrato anteri preços. Sendo assim, dada a importância atual de ter-se na solução de antivírus juntamente com a funcionalidade de EI 3 - Ao analisar o Parecer ASJUR, foram realizados diversos apontamentos que boa parte deles tinham como como por exemplo: • Necessidade de inclusão de plano de implantação para início e fim dos trabalhos; • Disciplina a forma de como deveria ser realizada a transferência de conhecimento; • Foram realizados apontamentos sobre a forma de como deveria ser exigido o Atestado de Capacidade Técn • Foi exigido que a unidade técnica estabelecesse os parâmetros para caracterização de suficiência do se avaliação para aprovação e questionário de avaliação a ser respondido pelos servidores treinados; • Foram recomendadas alterações na redação de diversos itens, com o intuito de deixar mais clara para os lic

XII – Apresente os indicadores para avaliar a economicidade, a eficácia e a efetividade:

Os softwares modernos de antivírus podem proteger contra:

- objetos maliciosos Browser Helper (BHOs);
- sequestradores de navegadores;
- ransomware;
- keyloggers;
- backdoors;
- rootkits;
- cavalos de tróia;
- worms;
- dialers;
- fraudtools;
- adware e spyware.

Também incluem proteção contra ameaças virtuais, tais como URL's infectadas e maliciosas, spam, fraude e ataques de p persistentes avançadas (APT).

Devido ao grande número de funcionalidades disponibilizadas pelos atuais fabricantes, a solução de antivírus passou a ser cha proteção a servidores de rede.

O termo endpoint também é muito utilizado para se referir a estações de trabalho e notebooks.

Uma das camadas de proteção é realizada pelo sistema de antimalware, atualmente chamado de sistema de proteção de esta segurança das estações de trabalho, notebooks, dispositivos mobile e sistemas de datacenters oferecendo proteção em tempo re ransomwares, além de fornecerem opções avançadas de segurança como o bloqueio de dispositivos e análise de ameaças não conhecid

Esta contratação visa atender:

A contratação visa atender as necessidades de proteção dos microcomputadores, notebooks e equipamentos servidores da Ju de destruição/alteração (parcial ou total) das atividades realizadas rotineiramente pelos usuários da rede da Justiça Eleitoral. Os vírus acabam por infectar dos os computadores que não estiverem com um sistema de proteção adequada com atualizações constantes.

Benefícios Esperados:

Os principais benefícios esperados com esta proposta de contratação são:

a)Manter o ambiente computacional da Justiça Eleitoral seguro;

b)Identificação de falhas de segurança de forma rápida;

c)Monitoramento contínuo dos serviços;

d)Proteção dos usuários, da instituição e da propriedade intelectual.

XIII – Indicação orçamentária:

A despesa correrá por conta do Programa 20 GP, cuja disponibilidade será informada posteriormente pela Secretaria de Planejament

XIV – Observações:

Informamos que a referida contratação não se enquadra nas previsões do Decreto nº 7.174/2010 tendo em vista tratar-se de

XV – Assinatura do servidor ou da equipe de planejamento da contratação responsável pela elaboração deste documento:

IVANILDO FERREIRA GOMES
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **01/09/2021, às 16:30**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

ISRAEL JOSÉ SZERMAN
ASSISTENTE IV

Documento assinado eletronicamente em **01/09/2021, às 16:30**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.