ESTUDOS TÉCNICOS / 2022 - NSCIB

1. IDENTIFICAÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

SOLUÇÃO DE TI	
NOME DA SOLUÇÃO DE TI:	SOLUÇÃO DE FERRAMENTA DE SEGURANÇA PARA SERVIDORES LINUX
ÁREA DEMANDANTE:	STI/CODIN
E-MAIL DO DEMANDANTE:	antonio.sousa@tre-pi.jus.br
TELEFONE DO DEMANDANTE:	86 2107 9826

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

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.

3. MOTIVAÇÃO / JUSTIFICATIVA

A aquisição da solução visa proteger os servidores de rede contra ameaças conhecidas como: objetos maliciosos browser helper (BHO), sequestradores de navegadores, ransomware, keyloggers, backdoors, rootkits, cavalos de troai, worms, dialers, fraudtools, adware e spyware. Também inclui proteção contra ameaças virtuais, tais como URLs infectadas e maliciosas, spam, fraude e ataques de phishing, identidade online (privacidade), ataques bancários online, ameaças persistentes avançadas (APT).

O não atendimento da necessidade trará para a rede da JE o risco de infecções causadas pelas ameaças relatadas acima, resultando em danos temporários e/ou permanentes aos sistemas críticos da JE e também desprotegendo toda a rede da JE do país, servindo como uma porta aberta para as ameaças virtuais.

Ainda assim, essa contratação é parte da Contratação dos Serviços Nacionais de Cibersegurança, definidos na Estratégia Nacional de Cibersegurança do TSE, e ainda na Estratégia Nacional de Segurança Cibernética e da Informação do Poder Judiciário, Resolução CNJ 396/2021 (*https://www.cnj.jus.br/cnj-regulamenta-estrategia-nacional-contra-ataques-ciberneticos-ao-judiciario/*). Faz parte também da Carteira de Projetos Estratégicos do TSE (*https://www.tse.jus.br/transparencia-e-prestacao-de-contas/carteira-de-projetos-estrategicos*).

4. RESULTADOS ESPERADOS

Com esta contratação pretende-se assegurar que os serviços de TIC sejam prestados de forma satisfatória, protegendo os servidores de rede e mitigando as ameças que possam comprometer a segurança de toda a rede de dados da JE do país.

5. REQUISITOS DE NEGÓCIO

5.1 – Requisitos funcionais (Necessidades de negócio)

NECESSIDADE 1				
Proteção avançada antimalware para servidores de rede, execução de aplicações maliciosas, realizar análise de bloqueio de aplicações baseada em comportamento, monitorar atividades de criptografia, proteção contra ataques 0Day e proteção para a solução de correio eletrônico.				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Proteção dos serviços críticos de TI contra ameaças virtuais, malwares e ramsonwares.	1	SEINF	STI
		2	NSCIB	STI
...				

5.2 – Requisitos não-funcionais

ID	TIPO	REQUISITO
1	Requisitos de capacitação	1. A contratação deve prover a transferência de conhecimento para operacionalizar a ferramenta.

2	Requisitos Legais	Devem-se observar as normas: 1. Lei n° 8.666, de 21 de junho de 1993, que institui normas para licitações e contratos da Administração Pública. 2. Lei n° 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação. 3. Decreto n° 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal e faz exigência contratual de comprovação da origem dos bens importados oferecidos pelos licitantes 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. 4. Resolução CNJ nº 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). 5. Resolução CNJ n° 370, de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação do Poder Judiciário (ENTIC-JUD). 6. Resolução TSE nº 23.234, de 15 de abril de 2010, que dispõe sobre regras e diretrizes para a contratação de serviços no âmbito da Justiça Eleitoral. 7. Orientação Técnica n° 01 TiControle, de 12 de março de 2008, que dispõe sobre boas práticas para a estimativa de preços na contratação de bens e serviços de TI. 8. Resolução TRE-PI nº 356/2017, de 19 de dezembro de 2017, que estabelece a Política de Segurança da Informação (PSI) do Tribunal Regional Eleitoral do Piauí. 9. Lei nº 10.520/2002; Decretos nºs 5.450/2005, 8.538/2015, 7.892/2013 e demais normas pertinentes. 10. Portaria Presidência Nº 423/2018, de 23 de abril de 2018, que dispõe sobre a regulamentação do procedimento de salvaguarda de dados no âmbito do TRE-PI.
3	Requisitos de Manutenção	não se aplica.
4	Requisito Temporal	1. suporte e garantia de atualização por no mínimo 60 meses.
5	Requisitos de Segurança da Informação	1. A CONTRATADA deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com o TRE-PI, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizado pelo TRE-PI. 2. A CONTRATADA deverá fornecer à CONTRATANTE todas as informações relevantes (configurações e regras de segurança) a respeito de equipamentos implantados na rede da CONTRATANTE. 3. O TRE-PI terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação. 4. A CONTRATADA deverá respeitar as normas de segurança estabelecidas pela CONTRATANTE durante a realização de atividades no ambiente desta. 5. Os equipamentos que forem submetidos ao serviço de garantia, deverão ser corretamente manutenidos de modo a garantir a disponibilidade e integridade das informações nele contidas. 6. A manutenção deverá ser realizada, preferencialmente, nas dependências do Tribunal. Havendo necessidade de remoção do equipamento para as dependências da empresa CONTRATADA, as despesas de transporte, seguros e embalagens, correrão por conta da empresa CONTRATADA. 7. No caso de retirada de qualquer equipamento, a empresa CONTRATADA deverá assinar Autorização para saída de material e Termo de Responsabilidade e Devolução se responsabilizando integralmente pelo equipamento (hardware e software), enquanto o mesmo estiver em suas dependências ou em trânsito sob sua responsabilidade. 8. Na retirada do equipamento, o CONTRATANTE deverá migrar o repositório de backup para outro equipamento ou fitas magnéticas, apagando o repositório de backup logo em seguida. 9. Somente os técnicos da empresa CONTRATADA, ou pessoas a quem ela autorizar por escrito, poderão executar os serviços de manutenção. Os técnicos, ou pessoas autorizadas pela empresa CONTRATADA, deverão apresentar, no ato do atendimento, credenciamento (crachá da empresa) e documento de identidade pessoal (RG), para efetuarem qualquer serviço nas dependências no Tribunal.
6	Requisitos Sociais, Ambientais e Culturais	1. Todos os manuais e guias de instruções deverão estar redigidos em língua portuguesa do Brasil e/ou inglês americano.
7	Requisitos de Desempenho	Definidos nas especificações dos requisitos tecnológicos.

5.3 – Requisitos tecnológicos

ID	TIPO	REQUISITO

1	Requisitos da Arquitetura Tecnológica	1. 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. 2. 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. 3. 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). 4. Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host. 5. Proteger de forma automática e transparente contra brechas de segurança descobertas interrompendo somente o tráfego malicioso. 6. Possuir a capacidade de detectar e bloquear ataques em aplicações web tais como: SQL Injection e Cross-Site Scripting dentre outros. 7. 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. 8. 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. 9. Operar como firewall de host statefull bidirecional, monitorando as comunicações nos servidores protegidos. 10. Possuir a capacidade de controlar o tráfego baseado no Endereço MAC, Frame Types, Tipos de Protocolos, Endereços IP e intervalo de portas. 11. 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. 12. 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. 13. Possuir a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão. 14. 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. 15. Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, os seguintes sistemas operacionais e aplicações: 1. Windows Server 2003 ou superiores (32 e 64 bits); 2. Linux Red Hat e suas variantes, CentOs, Debian e suas variantes nas versões (32 e 64 bits); 3. 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. 16. A solução deverá suportar a tecnologia hiperconvergente Nutanix. 17. Possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque. 18. Possibilitar a criação de regras customizadas, para proteger aplicações desenvolvidas pela Justiça Eleitoral. 19. 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. 20. 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. 21. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLAN's ou Switches. 22. Detectar ameaças avançadas no ambiente cibernético. 23. Corrigir falhas antes que o erro aconteça. 24. Monitorar continuamente os endpoints, quer estejam online ou offline. 25. Armazenar eventos e incidentes de malwares no endpoint. 26. Possuir capacidade de resposta em tempo real. 27. Promover a unificação das informações dos endpoints. 28. Dar maior visibilidade do ambiente de TI. 29. Integrar-se com as demais soluções de segurança. 30. Usar whitelists e blacklists.

2	Requisitos do Projeto de Implantação da solução de TI	1. 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; 2. A instalação da solução deverá ser realizada sem causar indisponibilidade do ambiente; 3. O processo de instalação da solução deverá ser acompanhado por servidores da Contratante; 4. Para garantir que a instalação não afetará o ambiente da Contratante, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante; 5. 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; 6. A instalação da solução no ambiente da Contratante não poderá interferir no bom funcionamento de outros sistemas previamente instalados
3	Requisitos da Garantia e Manutenção	1. suporte e garantia de atualização por no mínimo 60 meses.

4	Requisitos de Capacitação	1. 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. 2. 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). 3. O treinamento deverá ocorrer em dias úteis e em horário comercial. 4. A transferência de conhecimento deverá ser realizada de forma remota ou poderá ser realizado nas dependências do Tribunal Regional Eleitoral, conforme decisão do CONTRATANTE. 5. Cada turma referente a transferência de conhecimentos será compostas de: 1. no mínimo 3 (três) e no máximo 7 (sete) alunos. 2. 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. 6. 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. 7. 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. 8. 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. 9. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês). 10. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária. 11. 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. 12. Será considerado como satisfatório o percentual de aprovação acima de 70% (setenta por cento). 13. 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. 14. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelo fabricante dos softwares da solução ofertada.
5	Requisitos de Experiência Profissional da Equipe Técnica	1. A equipe deverá ser composta por técnicos qualificados e certificados pelo fabricante dos softwares da solução ofertada.
6	Requisitos de Formação da Equipe Técnica	1. certificação dos profissionais na solução ofertada.
7	Requisitos da Metodologia de trabalho	não se aplica.
8	Requisitos de Segurança sob o ponto de vista Técnico	não se aplica.

5.4 – Outros requisitos

ID	TIPO	REQUISITO
1		
...		

6. IDENTIFICAÇÃO DAS SOLUÇÕES DISPONÍVEIS

SOLUÇÃO 1	**NOME DA SOLUÇÃO:**	Adquirir a Solução de Antivírus com EDR/XDR por meio da adesão a ATA do TSE
	DESCRIÇÃO:	Aquisição de 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.
	FORNECEDOR(ES):	não se aplica
	ENTIDADE:	não se aplica
	VALOR:	R$ 230,00 anuais, totalizando R$ 46.000,00 o valor total do contrato (5 anos)
SOLUÇÃO 2	**NOME DA SOLUÇÃO:**	
	DESCRIÇÃO:	
	FORNECEDOR(ES):	
	ENTIDADE:	
	VALOR:	
SOLUÇÃO 3	**NOME DA SOLUÇÃO:**	
	DESCRIÇÃO:	
	FORNECEDOR(ES):	
	ENTIDADE:	
	VALOR:	

7. DETALHAMENTO DAS SOLUÇÕES E ALTERNATIVAS EXISTENTES

REQUISITO	ID DA SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	X		
	2			
	3			
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Eleitoral?	1	X		
	2			
	3			
A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2			
	3			
A Solução é um software livre ou software público?	1		X	
	2			
	3			
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1			X
	2			
	3			
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			X
	2			
	3			
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?	1			X
	2			
	3			

8. ANÁLISE E COMPARAÇÃO DOS CUSTOS TOTAIS DA DEMANDA

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.

Item	Fornecedor	Descrição	Qtd. Registrada	Vlr. Unit. Anual (R$)	Vlr. Unit. (60 meses)(R$)	Valor Global (R$)(60 meses)
1	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	220,00	1.100,00	220.00,00

Item	Fornecedor	Descrição	Qtd. Registrada	Vlr. Unit. Anual (R$)	Vlr. Unit. (60 meses)(R$)	Valor Global (R$)(60 meses)
2	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	124,65	623,25	124.650,00
3	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	137,02	655,10	131.020,00
4	ARP 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	46,00	230,00	46.000,00

9. SOLUÇÃO ESCOLHIDA

9.1 – Identificação

NOME:	Adquirir a Solução de Antivírus com EDR/XDR por meio da adesão a ATA do TSE		
JUSTIFICATIVA:	Conformidade com os requisitos tecnológicos, instalação e configuração sem ônus para o Tribunal, além de repasse tecnológico;		
DESCRIÇÃO:	Aquisição de 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.		
BENS E SERVIÇOS	**ID**	**BEM / SERVIÇO**	**VALOR ESTIMADO**
	1	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.	R$ 46.000,00
	...		

9.2 – Alinhamento com as necessidades de negócio

ID	FUNÇÃO	NECESSIDADE DO NEGÓCIO
1	Ferramenta com ação preventiva e de recuperação contra ataques virtuais, para servidores Linux e Windows.	Proteção dos serviços críticos de TI contra ameaças virtuais, malwares e ramsonwares.
...		

9.3 – Benefícios esperados

ID	TIPO	BENEFÍCIOS
1	Segurança e integridade	Assegurar os sistemas e arquivos contra ataques virtuais e eventual ataque a integridade dos dados.
...		

9.4 – Justificativa de não-conformidade

ID	SOLUÇÃO	JUSTIFICATIVA

10. AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO PARA EXECUÇÃO CONTRATUAL

ID	TIPO DE NECESSIDADE	SIM	NÃO	DESCRIÇÃO
1	Infraestrutura Tecnológica	X		Verificar a capacidade do Cluster de aplicações (Blade) para a criação de novas máquinas virtuais para execução dos serviços; verificar licenças disponíveis do Windows Server para uso dos serviços;
2	Infraestrutura Elétrica		X	Não se aplica
3	Logística de implantação		X	Não se aplica

4	Espaço Físico		X	Não se aplica
5	Mobiliário		X	Não se aplica
6	Impacto ambiental		X	Não se aplica

11. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

DESCRIÇÃO DOS RECURSOS NECESSÁRIOS PARA SUPORTAR A CONTRATAÇÃO DA SOLUÇÃO		
11.1. Recursos Materiais		
Item	**Descrição**	
1	Todos os softwares e instruções para o funcionamento da solução serão fornecidos pela contratada.	
...		
11.2. Recursos Humanos		
Item	**Função**	**Formação**
1	Gestor do Contrato	Definidos em Portaria TRE-PI
2	Fiscal Técnico	Definidos em Portaria TRE-PI
3	Analista de Redes	Conhecimento da infraestrutura de redes e serviços de TI do TRE-PI.

12. ESTRATÉGICA DE CONTINUIDADE CONTRATUAL

IDENTIFICAÇÃO DE EVENTOS QUE POSSAM CAUSAR INTERRUPÇÃO CONTRATUAL			
Evento	**Descrição**	**Ação de Contingência**	**Responsável**
1	Não entregar ou entregar o serviço fora do prazo estabelecido durante a contratação.	Multa / Considerar inexecução parcial ou total do objeto	SAOF
2	Em garantia, corrigir ou substituir o serviço fora do prazo estabelecido.	Multa / Considerar inexecução parcial ou total do objeto	STI
3	Não entregar os serviços adquiridos.	Multa / Considerar inexecução parcial ou total do serviço. Realizar novo processo para aquisição; Atender a demanda a ser suprida com serviços já existentes nas unidades	STI

13. AÇÕES PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Item	Ação	Responsável	Data Início	Data Fim
1	Será verificado, 180 (cento e oitenta) dias do término da vigência da garantia do serviço a possibilidade de extensão da garantia.	NSCIB	180 (cento e oitenta) dias do término da vigência	Data da vigência contratual.
...				

14. ESTRATÉGIA DE INDEPENDÊNCIA

14.1. Transferência de Conhecimento Tecnológico		
Item	**Informações que deverão ser transmitidas pela Contratada**	**Forma de transferência do Conhecimento**
1	Configurações específicas dos serviços adquiridos	Mídias e manuais.
...		
14.2. Direitos de Propriedade Intelectual e Autorais		
Item	**Cláusulas segundo a lei Nº 9.610, de 19 de fevereiro de 1998.**	
1	Não se aplica.	
...		

15. ANÁLISE DE RISCOS

15.1 – Riscos do processo de contratação (identificar os riscos que podem comprometer o processo de contratação, resultando em atrasos ou em comprometimento do processo de contratação – IN04, art. 16, I)

RISCO 1	PROBABILIDADE

NÃO CUMPRIMENTO DO PRAZO DE ENTREGA PELA CONTRATADA					(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Necessidade de utilização de computadores com antivirus desatualizados, podendo causar infecções e/ou epidemias de virus na JE do país.	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Acompanhar rigorosamente o processo de contratação; Interceder junto à contratada a fim de priorizar a entrega dos serviços	(X) 1-Mitigação ( ) 2-Contingência	Integrante demandante	CODIN
2		( ) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto		( ) 1-Mitigação ( ) 2-Contingência		

15.2 – Riscos da solução de TI escolhida (identificar os riscos que podem fazer com que, após o serviço ter sido contratado, o mesmo não atenda às necessidades do negócio especificadas – IN04, art. 16, II)

RISCO 1					**PROBABILIDADE**	
Solução não oferecer proteção eficiente contra ataques avançados.					(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Ocorrência de infecção por virus e demais malwares, e ineficiência ao mitigá-la colocando em risco a rede da JE do país.	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Acompanhamento constante da atualização da solução, além de acionamento do suporte da contratada. Acionamento dos canais de suporte da contratada.	(X) 1-Mitigação ( ) 2-Contingência	NSCIB	CODIN
		( ) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto		( ) 1-Mitigação ( ) 2-Contingência		

16. ESTRATÉGIA PARA CONTRATAÇÃO

16.1. SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (Res. CNJ 182/2013, art. 16)

16.1.1 – DEFINIÇÃO (NATUREZA DO OBJETO) DA SOLUÇÃO (critérios que serão usados para definir o tipo de contratação, modalidade de licitação, etc: inovação tecnológica ou serviço/bem comum; necessidade pontual ou contínua- Res. CNJ 182/2013, art. 16, IV)	
Critério	**Atendimento da Solução**
É possível especificar o serviço usando parâmetros usuais de mercado?	SIM
É possível medir o desempenho da qualidade usando parâmetros usuais de mercado?	SIM
O objeto da contratação se estende necessariamente por mais de um ano?	SIM
O objeto da contratação é essencial para o negócio?	SIM

16.1.2 – PARCELAMENTO E ADJUDICAÇÃO DA CONTRATAÇÃO (justificar se é técnica e economicamente viável dividir a solução a ser contratada. Informar se o objeto pode ou não ser dividido em itens ou até mesmo em grupos. Em caso de divisão, verificar se há prejuízo nos resultados finais a serem obtidos. De acordo com o parcelamento do objeto, informar se a adjudicação pode ou não ser realizada para mais de um fornecedor. Justificar a escolha. Esse item não se aplica aos casos de Dispensa ou Inexigibilidade - (Res. CNJ 182/2013, art. 16, II e III)
NÃO SE APLICA.

16.2. RESPONSABILIDADES DA CONTRATANTE E DA CONTRATADA

16.2.1 – DEVERES E RESPONSABILIDADES DA CONTRATANTE (deveres e responsabilidades da contratante que comporão o contrato)	
ID	**Dever / Responsabilidade**

1	Levar ao conhecimento da CONTRATADA, por escrito, qualquer fato extraordinário ou anormal que ocorrer na execução do objeto desta proposição, bem como imperfeições, falhas ou irregularidades constatadas no objeto pactuado, para que sejam adotadas as medidas corretivas necessárias. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA. Verificar e atestar as faturas da CONTRATADA. Efetuar o pagamento devido pela execução dos serviços, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas no Termo de referência.

16.2.2 – DEVERES E RESPONSABILIDADES DA(S) CONTRATADA(S) (deveres e responsabilidades da(s) contratada(s) que comporão o contrato. A(s) contratada(s) não poderá(ão) se eximir dessas responsabilidades, mesmo havendo subcontratação - (IN04, art. 15, II)

ID	Dever / Responsabilidade
1	A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus, os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda: Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos. Receber e assinar o instrumento que formalizará a contratação, no prazo máximo de **05 (cinco) dias úteis**, contados a partir de sua convocação por este Tribunal, sob pena de decair seu direito à contratação, sujeitando-se às penalidades previstas no art. 7º da Lei nº 10.520/2002 e no art. 87 da Lei n.º 8.666/93, podendo o TRE aplicar-lhe a multa de até 15% (quinze por cento) do valor total dos itens que lhe foram adjudicados; Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados. Deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com o TRE-PI, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizado pelo TRE-PI. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos; A CONTRATADA deverá respeitar as normas de segurança estabelecidas pela CONTRATANTE durante a realização de atividades no ambiente desta. A CONTRATADA deverá: a) prover assistência técnica no território brasileiro; b) dispor de um número telefônico para suporte técnico e abertura de chamados técnicos, c) apresentar tempo de resposta aos chamados abertos em até no máximo 24 horas, para problemas críticos, 48 h para problemas urgentes e 3 dias para problemas normais, conforme definição que constará de Termo de Referência; d) possuir um sistema de atendimento de suporte via Chat, 0800 ou através da Internet; Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação; Não transferir a terceiros, total ou parcialmente, o objeto desta licitação, nem subcontratar qualquer dos serviços a que está obrigada sem prévio assentimento por escrito do TRE-PI.

16.3 INDICAÇÃO DOS TERMOS CONTRATUAIS (IN04, art. 15, III)

16.3.1 – PROCEDIMENTOS E CRITÉRIOS DE ACEITAÇÃO (IN04, art. 15, III, a)

ID	**Etapa / Fase / Item** (em qual etapa, fase ou item do projeto será aplicada a mensuração)	**Indicador** (qual será o indicador mensurado. Qual será a unidade de medida a ser avaliada)	**Valor Mínimo Aceitável** (valor mínimo aceitável daquele item de mensuração)
1	Aceitação da proposta	Planilha de composição de custos	Valores mínimos exigidos no Edital
2	Execução contratual	Indicadores definidos no Termo de Referência	Valores mínimos exigidos no Termo de Referência

16.3.2 – FORMA DE PAGAMENTO (modo ou percentual que será pago por cada entrega em função do resultado a ser obtido -IN04, art. 15, III, e)

O pagamento será efetivado em até 10 dias após a protocolização da Nota Fiscal no Protocolo Geral do TRE-PI ou envio por email, e certificação do recebimento dos serviços pelo gestor do contrato.

16.3.3 – CRONOGRAMA DE EXECUÇÃO FÍSICO-FINANCEIRA (IN04, art. 15, III, f)			
ID	**Entrega** (listagem do item ou serviço a ser entregue. Esta entrega pode ser parcelada ou integral)	**Data de Entrega**	**Percentual a ser Pago**
1	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.	Até 10 dias corridos após recebimento da ordem de serviço.	20%
2	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.	Até 10 dias corridos após recebimento da ordem de serviço.	20%
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.	Até 10 dias corridos após recebimento da ordem de serviço.	20%
4	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.	Até 10 dias corridos após recebimento da ordem de serviço.	20%
5	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.	Até 10 dias corridos após recebimento da ordem de serviço.	20%
Total:			

16.3.4 – MECANISMOS FORMAIS DE COMUNICAÇÃO (IN04, art. 15, III, g)				
Função de Com. 1 (listagem do que deverá ser contemplado neste mecanismo de comunicação):	Assinatura de contrato, emissão de ordem de fornecimento, emissão de notas fiscais.			
Documento (nome do documento a ser entregue)	**Emissor**	**Destinatário**	**Meio** (forma com que o documento deverá ser produzido e entregue)	**Periodicidade** (frequência que os documentos deverão ser emitidos e entregues pela contratada ou pela administração)
Aditivo/Contrato	Contratante	Contratada	Eletrônico	uma vez
Nota Fiscal	Contratada	Contratante	Físico/Eletrônico	uma vez
Notificação	Contratante	Contratada	Eletrônico	Quando necessário
E-mail	Contratante	Contratada	Eletrônico	Quando necessário

16.3.5 – REGRAS PARA APLICAÇÃO DE MULTAS E SANÇÕES (IN04, art. 15, III, h)		
ID	**Ocorrência** (descrição clara das situações em que se caracterizará a infração a algum termo contratual. Devem ser descritas as não conformidades, ou outras situações ou ocorrências em que serão propostas sanções a serem aplicadas pela Área Administrativa)	**Sanção / Multa** (descrição da sanção/multa a ser aplicada de acordo com cada situação ou ocorrência listada. As multas e sanções devem ser proporcionais ao impacto que a ocorrência provocará no órgão e aos casos de reincidência das ocorrências)
1	Inexecução total ou parcial do contrato	A empresa registrada ficará sujeita, assim como as integrantes dos cadastro de reserva, que convocadas, não honrarem o compromisso assumido sem justificativa aceita pela Administração, nos casos de inexecução total ou parcial de suas obrigações, às sanções previstas no Capítulo XIV do Edital de Licitação do TSE n.° 84/2021, assegurados o contraditório e a ampla defesa, sem prejuízo do ressarcimento dos danos porventura causados à Administração. Endereço para comunicação: Seção de Almoxarifado e Patrimônio – SEALP, Tribunal Regional Eleitoral do Piauí, Praça Des. Edgar Nogueira, S/N – Centro Cívico, bairro Cabral, Teresina-PI, CEP 64000-920, fones: (086) 2107-9811/9787, e-mail: sealp@tre-pi.jus.br;

16.4. CRITÉRIOS TÉCNICOS DE JULGAMENTO DAS PROPOSTAS (IN04, art. 15, VII)

16.4.1 – CRITÉRIOS DE SELEÇÃO			
(X) Licitação ( ) Registro de Preço ( ) Dispensa de licitação ( ) Inexigibilidade de licitação			
Modalidade:	Pregão	**Tipo:**	Menor Preço por item
Justificativa: (obrigatório se for dispensa ou inexigibilidade de licitação)	Não se aplica.		

16.5. INDICAÇÃO DA EQUIPE DE GESTÃO DA CONTRATAÇÃO (ou comissão de recebimento de bens) (Res. CNJ 182/2013, art. 16, VIII)

Gestor do Contrato:	ANTONIO MANOEL SILVEIRA DE SOUSA	Telefone:	86 2107 9826
E-mail do Gestor do Contrato:	antonio.sousa@tre-pi.jus.br	Setor:	CODIN
Fiscal Demandante:		Telefone:	
E-mail do Fiscal Demandante:		Setor:	
Fiscal Técnico:	LEONARDO SARAIVA E SILVA	Telefone:	86 2107 9816
E-mail do Fiscal Técnico:	leonardo.saraiva@tre-pi.jus.br	Setor:	NSCIB
Fiscal Administrativo:	SIDNEI ANTUNES RIBEIRO	Telefone:	86 2107 9745
E-mail do Fiscal Administrativo:	sidnei.antunes@tre-pi.jus.br	Setor:	SELIC

17. ASSINATURAS

INTEGRANTE	NOME	ÁREA
Demandante:	ANTONIO MANOEL SILVEIRA DE SOUSA	CODIN
Técnico:	LEONARDO SARAIVA E SILVA	NSCIB
Administrativo:	SIDNEI ANTUNES RIBEIRO	SELIC

Teresina, 16 de março de 2022.

Documento assinado eletronicamente por **Antonio Manoel Silveira de Sousa**, **Coordenador de Desenvolvimento e Infraestrutura**, em 30/03/2022, às 13:56, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Anderson Cavalcanti de Lima**, **Secretário de Tecnologia da Informação**, em 04/04/2022, às 12:35, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1468296** e o código CRC **F47E3BC5**.