TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Praça Desembargador Edgard Nogueira. S/Nº - Centro Civico - Bairro Cabral - CEP 64000920 - Teresina - PI

ESTUDOS TÉCNICOS / 2020 - CODIN

1. IDENTIFICAÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

SOLUÇÃO DE TI	
NOME DA SOLUÇÃO DE TI:	Aquisição de solução de gestão de vulnerabilidades
ÁREA DEMANDANTE:	Coordenadoria de Desenvolvimento e Infraestrutura
E-MAIL DO DEMANDANTE:	antonio.sousa@tre-pi.jus.br
TELEFONE DO DEMANDANTE:	(86) 2107-9762

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Contratação de solução de gestão de vulnerabilidades de segurança nos ativos de TI, serviços e sistemas de TI que rodam no ambiente web.

3. MOTIVAÇÃO / JUSTIFICATIVA

A dependência dos processos por recursos de tecnologia da informação aumenta a cada dia, fato do qual o setor governamental não é uma exceção.

Isso eleva a criticidade dos ativos de TI, sejam eles dados/informações, software ou hardware. Qualquer ativo que represente valor para a organização deve ser protegido contra vulnerabilidades que o torne indisponível, a exemplo do ocorrido com o STJ; que permita o vazamento de informações críticas ou mesmo que venha a afetar a imagem da organização.

Para isso, faz-se necessário que a Equipe de Tratamento de Incidentes de Rede realize suas atividades de forma pró-ativa e não apenas reativa.

Devido à complexidade da infraestrutura das organizações, a proteção aos ativos só é possível através de ferramentas automatizadas que permitam o monitoramento das vulnerabilidades de segurança antes que estas vulnerabilidades sejam exploradas.

Assim, faz-se necessária a aquisição de solução de gestão de vulnerabilidades que permita testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer brechas, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além de fornecer dados atualizados à Alta Gestão acerca da segurança da informação da organização.

4. RESULTADOS ESPERADOS

A solução de software deve ser capaz de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que a solução forneça relatórios para que seja possível o acompanhamento deste trabalho de identificação e mitigação de riscos.

5. REQUISITOS DE NEGÓCIO

5.1 – Requisitos funcionais (Necessidades de negócio)

NECESSIDADE 1				
Gerenciamento de Vulnerabilidades em Sistemas Operacionais				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Testar os hosts (físicos e virtuais), comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software	1	Carlos Alberto Ribeiro do Nascimento Junior	SEINF
		...		
...				

NECESSIDADE 2				
Emissões de Relatórios				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas	1	Carlos Alberto Ribeiro do Nascimento Junior	SEINF
		...		
...				

5.2 – Requisitos não-funcionais

ID	TIPO	REQUISITO
1	Requisitos de capacitação	A contratação deve possuir um item de repasse tecnológico com no mínimo 20 horas para capacitar os servidores da STI a operacionalizar a ferramenta.
2	Requisitos Legais	Não há
3	Requisitos de Manutenção	Não há requisitos de manutenção dos itens adquiridos, exceto quando houver mudança de versão do sistema operacional.
4	Requisito Temporal	5.2.4.1. Prazos 5.2.4.1.1. O licitante terá 5 (cinco) dias contados da assinatura do contrato para fornecer os softwares ou as subscrições contratadas; 5.2.4.1.2. O atraso não justificado deverá ser punido de acordo com as sanções aplicadas ao contrato.
5	Requisitos de Segurança da Informação	5.2.5.1. A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação do da Justiça Eleitoral (Resolução TSE Nº 23.501/2016), 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; 5.2.5.2. O Tribunal Regional Eleitoral da Piauí terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação; 5.2.5.3. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX). 5.2.5.4. 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.
6	Requisitos Sociais, Ambientais e Culturais	5.2.6.1. Logística Reversa 5.2.6.1.1. 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; 5.2.6.1.2. 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; 5.2.6.1.3. 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.
7	Requisitos de Desempenho	

5.3 – Requisitos tecnológicos

ID	TIPO	REQUISITO
1	Requisitos da Arquitetura Tecnológica	5.3.1.1. A solução deve estar licenciadas e inclusas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malware) para no mínimo 250 IPs; 5.3.1.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede; 5.3.1.3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT; 5.3.1.4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures); 5.3.1.5. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas; 5.3.1.6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score; 5.3.1.7. A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades; 5.3.1.8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades; 5.3.1.9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente; 5.3.1.10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características: 5.3.1.10.1. Por sistema operacional; 5.3.1.10.2. Por um determinado software instalado; 5.3.1.10.3. Por Ativos impactados por uma determinada vulnerabilidade. 5.3.1.11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language); 5.3.1.12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente; 5.3.1.13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual; 5.3.1.14. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades; 5.3.1.15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina

(machine learning) para analisar as características relacionadas a vulnerabilidades;
5.3.1.16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
5.3.1.16.1. CVSSv3 Impact Score;
5.3.1.16.2. Idade da Vulnerabilidade;
5.3.1.16.3. Se existe ameaça ou exploit que explore a vulnerabilidade;
5.3.1.16.4. Número de produtos afetados pela vulnerabilidade;
5.3.1.17. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo;

5.3.1.18. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga no SIEM;

5.3.1.19. Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;

5.3.1.20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;
5.3.1.21. Se for baseada em nuvem, a solução deve possuir conectores para, no mínimo, as seguintes plataformas:
a) Amazon Web Service (AWS);
b) Microsoft Azure;
c) Google Clound Platform.

5.3.1.22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV ou HTML;
5.3.1.23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
5.3.1.24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

5.3.1.25. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:

a. Execução de verificação completa do sistema (rede), adequada para qualquer host;
b. verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
c. Autenticação de hosts e enumeração de atualizações ausentes;
d. Execução de varredura simples para descobrir hosts ativos e portas abertas;
e. Utilização de um scanner para verificar aplicativos da web;
f. Avaliação de dispositivos móveis
g. Auditoria de configuração de serviços em nuvem de terceiros;
h. Auditoria de configuração dos gerenciadores de dispositivos móveis;
i. Auditoria de configuração dos dispositivos de rede;
j. Auditoria de configurações do sistema em relação a uma linha de base conhecida;
k. Detecção de desvio de segurança Intel AMT;
l. Verificação de malware nos sistemas Windows e Unix;

5.3.1.26. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
5.3.1.27. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:
a) Bancos de dados;
b) Hypervisors (no mímino VMWare ESX/ESXi);
c) Dispositivos móveis;
d) Dispositivos de rede;
e) Endpoints;
f) Aplicações;
5.3.1.28. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;

5.3.1.29. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
5.3.1.30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.
5.3.1.31. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.
5.3.1.32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
5.3.1.33. Configuração de segurança e acesso à gerência da solução:
a) Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

b) Os dados em transito devem usar ao menos o algoritimo TLS 1.2 de chave 2048 bits;

c) Os dados em transito devem ser criptografados ao menos com o algoritimo AES-128 bits;

d) Os algoritimos de hash devem usar ao menos o algoritimo SHA-256;

e) Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;

e) Os dados armazenados devem ser criptografados ao menos com o algoritimo AES-256 bits;

f) Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
g) A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;

h) A empresa contratada não deverá ter acesso a rede interna da contratante e todo trafego de dados deverá ser de saída e iniciado pelos scanners (on-premises).

5.3.1.34. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
5.3.1.35. Dos Relatórios:
5.3.1.35.1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
5.3.1.35.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
5.3.1.35.3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;
5.3.1.35.4. A solução deve suportar o envio automático de relatórios para destinatários específicos;
5.3.1.35.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
5.3.1.35.6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
5.3.1.35.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
5.3.1.35.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
5.3.1.36. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
5.3.1.37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
5.3.1.37.1. Hosts verificados sem credenciais;
5.3.1.37.2. Top 100 Vulnerabilidades mais criticas;
5.3.1.37.3. Top 10 Hosts infectados por Malwares;
5.3.1.37.4. Hosts exploráveis por Malwares;
5.3.1.37.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
5.3.1.37.6. Vulnerabilidades críticas e exploráveis;
5.3.1.37.7. Máquinas com vulnerabilidades que podem ser exploradas;
5.3.1.38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
5.3.1.39. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
5.3.1.40. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 250 IPs;
5.3.1.41. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
5.3.1.42. Deve permitir a configuração de vários painéis e widgets;
5.3.1.43. Deve ser capaz de medir e reportar ameaças;
5.3.1.44. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
5.3.1.45. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;
5.3.1.46. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
5.3.1.47. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades;
5.3.1.48. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

5.3.1.49. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
5.3.1.50. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
5.3.1.51. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou;
5.3.1.52. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
5.3.1.53. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
5.3.1.54. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;
5.3.1.55. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais;

5.3.1.56. A solução deve possuir módulo para realizar análise dinâmica em aplicações Web:

5.3.1.56.1 A solução deve possuir módulo para realizar varreduras de vulnerabilidades para no mínimo 5 aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC:

5.3.1.56.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;

		5.3.1.56.3. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS); 5.3.1.56.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal; 5.3.1.56.5. Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos: a) Cookies, Headers, Formulários e Links; b) Nomes e valores de parâmetros da aplicação; c) Elementos JSON e XML; d) Elementos DOM; 5.3.1.56.6. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação; 5.3.1.56.7. A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas; 5.3.1.56.8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças; 5.3.1.56.9. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web; 5.3.1.56.10. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário; 5.3.1.56.11. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares; 5.3.1.56.12. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões; 5.3.1.56.13. Deve ser capaz de instituir no mínimo os seguintes limites: a) Número máximo de URLs para crawling e navegação; b) Número máximo de diretórios para varreduras; c) Número máximo de elementos DOM; d) Tamanho máximo de respostas; e) Tempo máximo para a varredura; f) Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação Web; g) Número máximo de requisições HTTP(S) por segundo; 5.3.1.56.14. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual; 5.3.1.56.15. Deve suportar o envio de notificações por email; 5.3.1.56.16. Deverá ser compatível com avaliação de web services REST e SOAP; 5.3.1.56.17. A solução de análise deve suportar os seguintes esquemas de autenticação: a) Autenticação Básica (Digest); b) NTLM; c) Autenticação de Cookies; 5.3.1.56.18. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário; 5.3.1.56.19. A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades; 5.3.1.56.20. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações; 5.3.1.56.21. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências; 5.3.1.56.22. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação; 5.3.1.56.23. Serviço de Detecção de Malware: a) A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente; b) A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por malware; c) A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação específica, que serão exportados para os formatos XML, HTML ou PDF. 5.3.1.56.24. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações: a. WordPress; b. IIS 6.x e IIS 10.x; c. ASP 6; d. NET 2; e. Apache HTTPD 2.2.x e 2.4.x; f. Tomcat 6.x, 7.x, 8.x e superiores; g. Jetty 8 e superiores; h. Nginx; i. PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores; j. Java 1.5, 1.6, 1.7 e 1.8 e superiores; k. Jboss 4.x e 7.x e superiores; l. WildFly 8 e 10 e superiores; m. Plone 2.5.x e 5.2.1.41.x e superiores; n. Zope; o. Python 2.4.4 e superiores; p. J2EE; q. Ansible; r. Joomla; s. Moodle; t. Docker Conteiner; u. Elk; v. GIT; w. Grafana; e x. Redmine.
2	Requisitos do Projeto de Implantação da solução de TI	
3	Requisitos da Garantia e Manutenção	

		A garantia de atualização do software deve ser de, no mínimo, 60 (sessenta) meses, contados do dia seguinte ao vencimento do suporte em vigência dos itens constantes no portal do fabricante.
4	Requisitos de Capacitação	
5	Requisitos de Experiência Profissional da Equipe Técnica	
6	Requisitos de Formação da Equipe Técnica	
7	Requisitos da Metodologia de trabalho	
8	Requisitos de Segurança sob o ponto de vista Técnico	

5.4 – Outros requisitos

ID	TIPO	REQUISITO
1		
...		

6. IDENTIFICAÇÃO DAS SOLUÇÕES DISPONÍVEIS

SOLUÇÃO 1	**NOME DA SOLUÇÃO:**	Softwares livres OpenVas e Nmap
	DESCRIÇÃO:	Utilizar ferramentas livres ou gratuitas, como os softwares OpenVas e Nmap.
	FORNECEDOR(ES):	Comunidades Open Source e páginas específicas dos projetos.
	ENTIDADE:	
	VALOR:	0,00
SOLUÇÃO 2	**NOME DA SOLUÇÃO:**	Solução de Gestão de Vulnerabilidades On Cloud
	DESCRIÇÃO:	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por 60 meses.
	FORNECEDOR(ES):	Empresa: Service IT, Ferramenta: Qualys (1127024), proposta: **R$ 315.698,00;** Empresa: SERVIX, Tenable (1127028), proposta: **R$ 391.256,00;** e Empresa: Netconn,, Rapid7 (1127026), proposta: **R$ 716.112,50.** **Devido a grande disparidade de valor a proposta da empresa Netconn será desconsiderada.**
	ENTIDADE:	
	VALOR MÉDIO:	**R$ 353.477,00**
SOLUÇÃO 3	**NOME DA SOLUÇÃO:**	Solução de Gestão de Vulnerabilidades On premises
	DESCRIÇÃO:	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 meses ou de licença perpetua com suporte de 60 meses.
	FORNECEDOR(ES):	Empresa: SERVIX, Ferramenta:Tenable (1127028), proposta: **R$ 211.310,00** ; e Empresa: Netconn, Ferramenta: Rapid7 (1127026), proposta: **R$ 921.631,25** **Devido a grande disparidade de valor a proposta da empresa Netconn será desconsiderada.**
	ENTIDADE:	
	VALOR MÉDIO:	**R$ 211.310,00**

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	X		
	3	X		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Eleitoral?	1			X
	2	X		
	3	X		
A Solução está disponível no Portal do Software Público Brasileiro?	1			X
	2			X
	3			X
A Solução é um software livre ou software público?	1	X		
	2		X	

	3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1			X
	2			X
	3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			X
	2			X
	3			X
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			X
	3			X

8. ANÁLISE E COMPARAÇÃO DOS CUSTOS TOTAIS DA DEMANDA

As pesquisas de preços constantes neste processo deram-se a partir de estudos e pesquisas conduzidos por alguns Tribunais da Justiça Eleitoral e é resultado de trabalho colaborativo destes Regionais. As propostas foram solicitadas para atender aos Tribunais que manifestaram interesse na aquisição de solução de gestão de vulnerabilidades.

Os custos estimados da contratação são conforme tabela abaixo.

Soluções de TIC - propostas de possíveis fornecedores/pesquisa no mercado de TIC

COMPARAÇÃO DOS CUSTOS DAS PROPOSTAS ON CLOUD						
Item	Fornecedor	Descrição/Modelo	Quantidade Prevista	Quantidade Registrada	Valor Unitário	Valor Total
8.1	Comunidades	Softwares livres OpenVas e Nmap	0	0	R$ 0,00	R$ 0,00
8.2.1 - 02	Qualys (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.	1	1	R$ 212.040,00	R$ 212.040,00
8.2.2. - 03	Qualys (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 92.268,00	R$ 92.268,00
8.2.3. - 04	Qualys (on cloud)	Instalação e configuração.	1	1	R$ 6.890,00	R$ 6.890,00
8.2.4. -05	Qualys (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 4.500,00	R$ 4.500,00
8.2.5. -06	Qualys (on cloud)	4 Horas de Serviço Especializado.	0	50	R$ 1250,00	R$ 0,00
8.2	**TOTAL Qualys (on cloud)**	---------- ---------- ----------	----------	----------	----------	**R$ 315.698,00**
8.3.1	Rapid7 (on	Licenciamento de	1	1	R$ 257.075,00	R$ 257.075,00

-02	cloud)	plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.				
8.3.2-03	Rapid7 (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 411.037,50	R$ 411.037,50
8.3.3-04	Rapid7 (on cloud)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 38.000,00	R$ 38.000,00
8.3.4-05	Rapid7 (on cloud)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 10.000,00	R$ 10.000,00
8.3.5-06	Rapid7 (on cloud)	4 Horas de Serviço Especializado.	0	50	R$ 1000,00	R$ 0.000,00
8.3	**TOTAL Rapid7 (on cloud)**	----------	----------	----------	----------	**R$ 716.112,50**
8.4.1-02	Tenable (on cloud)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 36 meses de uso e suporte do fabricante	1	1	R$ 263.742,00	R$ 263.742,00
8.4.2-03	Tenable (on cloud)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte do fabricante.	1	1	R$ 107.850,00	R$ 107.850,00
8.4.3-04	Tenable (on cloud)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 11.322,00	R$ 11.322,00
8.4.4-05	Tenable (on cloud)	Repasse Tecnológico com período mínimo de 20 horas	1	1	R$ 8.342,00	R$ 8.342,00

8.4.5-06	Tenable (on cloud)	4 Horas de Serviço Especializado.	0	50	R$ 0,00	R$ 0,00
8.4	**TOTAL Tenable (on cloud)**	----------	----------	----------	----------	**R$ 391.256,00**

COMPARAÇÃO DOS CUSTOS DAS PROPOSTAS ON PREMISES (LICENÇAS PERPÉTUAS)						
Item	Fornecedor	Descrição/Modelo	Quantidade Prevista	Quantidade Registrada	Valor Unitário	Valor Total
8.5.1-02	Rapid7 (on premise)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.	1	1	R$ 257.075,00	R$ 257.075,00
8.5.2-03	Rapid7 (on premise)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 123.311,25 por aplicação	R$ 616.556,25
8.5.3-04	Rapid7 (on premise)	Instalação e configuração e repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 38.000,00	R$ 38.000,00
8.5.4-05	Rapid7 (on premise)	Repasse Tecnológico com período mínimo de 20 horas.	1	1	R$ 10.000,00	R$ 10.000,00
8.5.5-06	Rapid7 (on premise)	4 Horas de Serviço Especializado.	0	50	R$ 1000,00	R$ 0,00
8.5	**TOTAL Rapid7 (on premise)**	----------	----------	----------	----------	**R$ 921.631,25**
8.6.1-02	Tenable (on premise)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.	1	1	R$ 191.646,00	R$ 191.646,00

8.6.2-03	Tenable (on premise)	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	1	1	R$ 0,00	R$ 0,00
8.6.3-04	Tenable (on premise)	Instalação e configuração.	1	1	R$ 11.322,00	R$ 11.322,00
8.6.4-05	Tenable (on premise)	Repasse Tecnológico com período mínimo de 20 horas	1	1	R$ 8.342,0	R$ 8.342,00
8.6.5-06	Tenable (on premise)	4 Horas de Serviço Especializado.	0	50	R$ 0,00	R$ 0,00
8.6	**Tenable (on premise)**	---------- ---------- ----------	----------	----------	----------	**R$ 211.310,00**

De forma resumida temos a tabela a seguir apresenta as propostas que estão sendo consideradas na análise dos custos:

Proposta	Empresa	Solução	Valor Total
COMPARAÇÃO DOS CUSTOS DAS PROPOSTAS ON CLOUD			
1	Service IT	Qualys	**R$ 315.698,00**
3	SERVIX	Tenable	**R$ 391.256,00**
COMPARAÇÃO DOS CUSTOS DAS PROPOSTAS ON PREMISES (LICENÇAS PERPÉTUAS)			
6	SERVIX	Tenable	**R$ 211.310,00**

A solução 1 baseada em Software Livre atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos. Outro ponto desfavorável ao uso do Software Livre é que os relatórios fornecidos pela ferramenta não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

A solução 2 baseada em nuvem (cloud computing) apresenta facilidade de gerenciamento, valor de aquisição adequado e facilidade nas atualizações da solução que serão todas feitas pelo fabricante. Todas os requisitos de funcionalidades do projeto são atendidos por esse cenário. As soluções analisadas Qualys (VM e módulo WAS), Tenable (Tenable.io e módulo WAS) e Rapid7 (IVM e módulo IAS) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. **Porém como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são muito sensíveis não é recomendável estarem armazenados em uma nuvem na qual não temos o controle algum sobre acesso, armazenamento e segurança. O armazenamento de dados sensíveis em nuvem é ainda desaconselhado pela Norma Complementar 14 do Gabinete de Segurança Institucional da Presidência da República.**

A solução 3 baseada em gerenciamento em rede local do tribunal (On premises) fornecida pela Tenable apresenta um valor de aquisição adequado e menor do que a Solução 2 (On cloud). Apesar de a solução 3 (On premise) trazer o trabalho de atualização para a equipe de infraestrutura de rede, ela possui um menor risco de vazamento de dados sensíveis que são as vulnerabilidades dos ativos de TIC do Tribunal, pois os mesmos serão armazenados na rede local do Tribunal e não em nuvem pública. Todas os requisitos de funcionalidades do projeto também são atendidos por esse cenário. As soluções analisadas Tenable (Tenable.sc) e Rapid7 (Nexpose e módulo AppSpider) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. **Outro ponto favorável à solução 3 fornecida pela Tenable é o fato de que após o término do suporte a STI continuará a ter acesso a ferramenta embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades.**

Sendo assim, não resta outra alternativa para o TRE no momento senão a solução 3 baseada no gerenciamento em rede local do tribunal, tendo em vista o menor preço da Solução 3 e o fato de fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web sem armazenar em nuvem pública os dados sensíveis que são as vulnerabilidades dos ativos de TIC do tribunal.

Esclarecemos que inicialmente, manifestamos interesse em adquirir licenciamento para 250 IPs, por 3 anos de uso, mas ao final quando verificamos o preço oferecido pela empresa SERVIX Informática Ltda, que apresentou a solução Tenable, resolvemos requerer o licenciamento para 5 anos de uso.

9. SOLUÇÃO ESCOLHIDA

9.1 – Identificação

NOME:	Solução de Gestão de Vulnerabilidades On premises (licenças perpétuas)		
JUSTIFICATIVA:	A solução escolhida além de apresentar o menor preço permite ao Tribunal continuar utilizando a ferramenta adquirida após os 5 anos de uso, porém sem o direito de realizar atualizações de versão e de novas vulnerabilidades.		
DESCRIÇÃO:	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 meses ou de licença perpetua com suporte de 60 meses.		
BENS E SERVIÇOS	**ID**	**BEM / SERVIÇO**	**VALOR ESTIMADO**
	1	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 60 meses de uso e suporte do fabricante.	R$ 191.646,00
	2	Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 60 meses de uso e suporte do fabricante.	0,00
	3	Instalação e configuração.	R$ 11.322,00
	4	Repasse Tecnológico com período mínimo de 20 horas	R$ 8.342,00
	5	4 Horas de Serviço Especializado.	0,00
	...	**TOTAL ESTIMADO:**	R$ 211.310,00

9.2 – Alinhamento com as necessidades de negócio

ID	FUNÇÃO	NECESSIDADE DO NEG
1	A solução é capaz de identificar vulnerabilidades catalogadas em diversos CVEs (*Common Vulnerabilities and Exposures*)	Gerenciamento de vulne Sistemas Operacionais
2	A solução é capaz de calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades	Aumentar o nível da seguran
3	A solução é capaz de gerar relatórios de acompanhamento para a Alta Gestão tomar conhecimento da evolução da gestão de vulnerabilidades do órgão	Emissões de relatórios

9.3 – Benefícios esperados

ID	TIPO	BENEFÍCIOS
1	Conformidade	Gerenciamento de vulnerabilidades, 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.
2	Confiabilidade	Utilização de ferramentas atualizadas contra ameaças cibernéticas
3	Disponibilidade	A eliminação de vulnerabilidades propiciará à rede do TRE-PI uma maior imunidade à ataques cibernéticos, aumentando sua resiliência e disponibilidade
4	Segurança	A eliminação de vulnerabilidades propiciará uma maior segurança dos dados e ativos do Tribunal
5	Padronização	Utilização de solução utilizada pelo TSE e TREs, possibilitando a troca de experiências
6	Orçamentária	Aquisição de solução com preço mais competitivo devido a compra em escala

9.4 – Justificativa de não-conformidade

ID	SOLUÇÃO	JUSTIFICATIVA
1	Softwares livres OpenVas e Nmap	Atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos
2	Solução de Gestão de Vulnerabilidades On Cloud	O armazenamento de dados sensíveis em nuvem é desaconselhado pela Norma Complementar 14 do Gabinete de Segurança Institucional da Presidência da República.

10. AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO PARA EXECUÇÃO CONTRATUAL

ID	TIPO DE NECESSIDADE	SIM	NÃO	DESCRIÇÃO
1	Infraestrutura Tecnológica		X	
2	Infraestrutura Elétrica		X	
3	Logística de implantação	X		Disponibilizar mão de obra especializada para implantação da solução e testes de configuração necessárias ao seu bom funcionamento.
4	Espaço Físico		X	
5	Mobiliário		X	
6	Impacto ambiental		X	

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	Não se aplica
...	

11.2. Recursos Humanos

Item	Função	Formação
1	Administrador de Redes	Conhecimento em configuração da rede de computares e segurança da informação
...		

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 objeto fora do prazo estabelecido durante a contratação.	Multa / Considerar inexecução parcial ou total do objeto	SAOF
2	Em garantia, corrigir ou substituir o objeto fora do prazo estabelecido	Multa / Considerar inexecução parcial ou total do objeto	SAOF
3	Em garantia, não fornecer as atualizações necessárias ao bom funcionamento da solução	Multa / Considerar inexecução parcial ou total do objeto	SAOF

13. AÇÕES PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Item	Ação	Responsável	Data Início	Data Fim
1	Os requisitos de negócio e os serviços de suporte serão cobertos pela garantia previstas no Termo de Referência. Durante esse período, a contratada será obrigada a fornecer todas as atualizações necessárias e manter os serviços ativos. No mínimo 180 (cento e oitenta) dias antes do encerramento do Contrato, será iniciado novo procedimento licitatório para substituição e/ou continuidade dos serviços da solução.	CODIN	01/06/2025	01/01/2026
...				

14. ESTRATÉGIA DE INDEPENDÊNCIA

14.1. Transferência de Conhecimento Tecnológico

Item	Informações que deverão ser transmitidas pela Contratada	Forma de transferência do Conhecimento
1	Formas de instalação, desinstalação e operacionalização	Treinamento
2	Resolução de inconsistências, dúvidas e adequações	Suporte

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	
Tempo excessivo na tramitação do processo de adesão					( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Impossibilidade de participação na IRP do TRE-PB	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Realizar contratação própria	( ) 1-Mitigação (X) 2-Contingência	Integrante Demandante	CODIN
2	Maior custo para contratação da solução	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Solicitar suplementação orçamentária	( ) 1-Mitigação ( ) 2-Contingência	Integrante Demandante	CODIN

RISCO 2	PROBABILIDADE
Não disponibilidade orçamentária para aquisição da solução escolhida	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto

ID	EFEITO	IMPACTO	AÇÃO DE RESPOSTA AO RISCO	TIPO DE AÇÃO	RESPONSÁVEL	ÁREA
1	Não contratação	( ) 1-Baixo (X) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Remanejamento de recursos de outras aquisições menos prioritárias	( ) 1-Mitigação (X) 2-Contingência	Integrante Demandante Integrante Administrativo	CODIN SAOF
2	Deixar a rede do TRE-PI vulnerável à ameaças cibernéticas	( ) 1-Baixo ( ) 2-Médio ( ) 3-Alto (X) 4-Muito alto	Solicitação de Orçamento	(X) 1-Mitigação ( ) 2-Contingência	Integrante Demandante	CODIN
4	Utilização de ferramentas/recursos open source	( ) 1-Baixo (X) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	Viabilizar outras camadas de segurança	( ) 1-Mitigação (X) 2-Contingência	Integrante Técnico	SEINF

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	
Serviços de suporte/garantia de baixa qualidade					(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**DANO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Solução funcionando inadequadamente ou base de vulnerabilidades desatualizada	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Acompanhar abertura de chamado e sugerir aplicação de multa à contratada, caso os prazos estabelecidos em edital não sejam atendidos	(X) 1-Mitigação ( ) 2-Contingência	Fiscal Técnico/Administrativo	SEINF

RISCO 2					PROBABILIDADE	
O software e produtos contratados não atendem completamente aos requisitos propostos para a aquisição					(X) 1-Baixo ( ) 2-Médio ( ) 3-Alto ( ) 4-Muito alto	
ID	**EFEITO**	**IMPACTO**	**AÇÃO DE RESPOSTA AO RISCO**	**TIPO DE AÇÃO**	**RESPONSÁVEL**	**ÁREA**
1	Não atendimento as demandas do negócio	( ) 1-Baixo ( ) 2-Médio (X) 3-Alto ( ) 4-Muito alto	Realização de prova de conceito da ferramenta antes de adquirir	(X) 1-Mitigação ( ) 2-Contingência	Integrante Técnico	SEINF

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. A solução visa gerenciar as vulnerabilidades de ativos que se forem exploradas por hackers poderá inviabilizar o acesso aos serviços e sistemas de TI críticos pra o negócio.

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)

A solução não é divisível, uma vez que é composta por elementos interdependentes, administrados coletivamente por uma única console central de gerenciamento.

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	16.2.1.1. Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA, necessários à execução do contratado; 16.2.1.2. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições dos equipamentos, fixando prazo para a sua correção de acordo com os definidos no presente Termo; 16.2.1.3. Verificar se os equipamentos estão de acordo com as especificações, podendo sustar, recusar, mandar fazer ou desfazer qualquer serviço que esteja em desacordo com as especificações deste documento; 16.2.1.4. Atestar a(s) notas fiscal(ais) apresentada(s) pela CONTRATADA após o recebimento definitivo dos equipamentos, conforme especificações descritas neste Termo de Referência; 16.2.1.5. Efetuar o pagamento nas condições, preços e prazos pactuados; 16.2.1.6. Acompanhar e fiscalizar o cumprimento das obrigações da contratada, determinando o que for necessário a regularização das falhas ou defeitos observados, ou ainda propor aplicações de penalidades e a sanções administrativas regulamentares e contratuais cabíveis, sempre que for o caso.

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	2.2.1. 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: a) Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos. b) Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto deste contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados. c) 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. d) 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; 2.2.2. A CONTRATADA deverá respeitar as normas de segurança estabelecidas pela CONTRATANTE durante a realização de atividades no ambiente desta. 2.2.3. 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 6 horas; d) possuir um sistema de atendimento de suporte via Chat, 0800 ou através da Internet; **e) dar garantia não inferior a 60 meses, a contar da data de emissão do Termo de Recebimento Definitivo;** 2.2.4. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

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	Configurações dos equipamentos/serviços ofertados	Valores mínimos exigidos no Edital.
...			

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 efetuado por meio de depósito bancário em conta corrente, até o 10º (décimo) dia útil a partir da apresentação da Fatura/Nota Fiscal, devidamente certificada pelo fiscal do contrato e processada na forma da legislação vigente.

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 para Gestão de vulnerabilidades on premises	Até 05(cinco) dias contados da assinatura do contrato	100%
...			
Total: R$ 211.310,00			

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)
Ata de Registro de Preços	Contratante	Contratada	Eletrônico	1 vez
Contrato	Contratante	Contratada	Eletrônico	1 vez
Ordem de Fornecimento	Contratante	Contratada	Eletrônico	1 vez
Nota Fiscal	Contratante	Contratada	Físico/Eletrônico	1 vez
Nota de Empenho	Contratante	Contratada	Eletrônico	1 vez

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	• Não assinar o contrato ou Ata de Registro de Preços • Deixar de entregar documentação exigida neste edital; • Apresentar documentação falsa; • Não manter a proposta; • Falhar ou fraudar na execução do contrato; • Comportar-se de modo inidôneo; • Fazer declaração falsa; • Cometer fraude fiscal.	Fundamentado no artigo 7º da Lei 10.520/2002, regulamentado pelo artigo 49 do Decreto n.º 10.024/2019, ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até 05 (cinco) anos, garantido o direito à ampla defesa
2	Faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante	Penalidade de advertência
3	• Atraso no cumprimento das obrigações assumidas contratualmente, que tenha acarretado prejuízos financeiros para o TRE-PI; • Entrega de objeto, em desacordo com a proposta aceita pela Contratante, sem prejuízo das demais sanções.	Suspensão temporária de participação em licitação e impedimento de contratar com o TRE-PI, p**or até 1 (um) ano,** se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato
4	• Entrega de objeto falso, seja como amostra ou como bem a ser entregue por ocasião de emissão de ordem de fornecimento, assim entendido, aquele em que houve manipulação para aparentar ser de outra marca/fabricante, ou ter características que originalmente não lhe pertençam, sem prejuízo das demais medidas cabíveis; • Não atendimento à solicitação de troca ou prestação de garantia do objeto, quando solicitado pela Contratante, no prazo fixado no edital • Cometimento de quaisquer outras irregularidades que acarretem prejuízo ao TRE-PI, ensejando a rescisão do Contrato por culpa da CONTRATADA; • Apresentação, ao TRE-PI, de qualquer documento falso ou falsificado, no todo ou em parte, com o objetivo de comprovar, durante a execução do Contrato, a manutenção das condições apresentadas na habilitação	Suspensão temporária de participação em licitação e impedimento de contratar com o TRE-PI, p**or até 2 (dois) anos,** se, por culpa ou dolo, prejudicar ou tentar prejudicar a execução do Contrato
5	Entrega do objeto com atraso	Multa moratória mensurada na forma de tabela a ser prevista no termo de referência, até o limite de 13% (treze por cento), calculada sobre o valor do objeto em atraso.

6	Inexecução total do contrato	Multa compensatória de 15% (quinze por cento) sobre o valor do objeto

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

16.4.1 – CRITÉRIOS DE SELEÇÃO			
( ) Licitação (X) Registro de Preço ( ) Dispensa de licitação ( ) Inexigibilidade de licitação			
Modalidade:	Licitação	**Tipo:**	Pregão Eletrônico
Justificativa: (obrigatório se for dispensa ou inexigibilidade de licitação)	Aquisição de bens e/ou serviços comuns pelo Sistema de Registro de Preços devido a contratação não ter sido contemplada com o orçamento necessário para o exercício 2020. Dessa forma, mais benéfico ao Tribunal, participar de Intenção de Registro de Preços proposta pelo TRE-PB de forma a lhe possibilitar a aquisição por um custo menor.		

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:	Antônio Manoel Silveira de Sousa	Telefone:	2107-9762
E-mail do Gestor do Contrato:	antonio.sousa@tre-pi.jus.br	Setor:	STI/CODIN
Fiscal Demandante:	Antônio Manoel Silveira de Sousa	Telefone:	2107-9762
E-mail do Fiscal Demandante:	antonio.sousa@tre-pi.jus.br	Setor:	STI/CODIN
Fiscal Técnico:	Carlos Alberto ribeiro do Nascimento Jr.	Telefone:	2107-9756
E-mail do Fiscal Técnico:	carlos.nascimento@tre-pi.jus.br	Setor:	STI/CODIN/SEINF
Fiscal Administrativo:	Sidnei Antunes Ribeiro	Telefone:	2107-9676
E-mail do Fiscal Administrativo:	sidnei.antunes@tre-pi.jus.br	Setor:	SAOF/COCONP/SELIC

17. ASSINATURAS

INTEGRANTE	NOME	ÁREA
Demandante:	Antônio Manoel Silveira de Sousa	STI/CODIN
Técnico:	Carlos Alberto ribeiro do Nascimento Jr.	STI/CODIN/SEINF
Administrativo:	Sidnei Antunes Ribeiro	SAOF/COCONP/SELIC

Teresina, 20 de novembro de 2020.

Documento assinado eletronicamente por **Carlos Alberto Ribeiro do Nascimento Junior**, **Técnico Judiciário**, em 23/11/2020, às 10:43, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Sidnei Antunes Ribeiro**, **Chefe de Seção**, em 23/11/2020, às 12:57, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Antonio Manoel Silveira de Sousa**, **Coordenador de Desenvolvimento e Infraestrutura**, em 23/11/2020, às 13:22, 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 **1126906** e o código CRC **02CA6F98**.