ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Termo de Referência – TR

AQSETIN2022015 – Solução de gestão e análise de vulnerabilidades de ativos

1. OBJETO DA CONTRATAÇÃO

1.1. É objeto da presente licitação a Contratação de empresa especializada em serviços de tecnologia da informação e comunicação, para fornecimento e instalação de **solução de gestão e análise de vulnerabilidades de ativos e aplicações web do TJCE.** A solução compreende a subscrição de licenças de software, incluindo a garantia de atualização das versões e o suporte técnico (24x7); consultoria especializada e capacitação, conforme condições, quantidades e exigências estabelecidas neste documento e seus anexos.

1.2. A contratação deverá compreender o período de 60 (meses). As especificações, funcionalidades e quantidades serão definidas e justificadas em momento oportuno, neste documento de estudo técnico.

1.3. Quantitativo

ID	Demanda Prevista	Quantitativo a ser Contratado
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	150
2	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	114
3	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	400

4	Suporte Técnico Especializado	24
5	Treinamento Técnico da Solução de Gerenciamento de Vulnerabilidades	8

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Motivação

2.1.1. A infraestrutura tecnológica do Poder Judiciário do Estado do Ceará é composta por ativos de rede; servidores, estações de trabalho e notebooks; servidores em Cloud; contêineres e aplicações Web e API;

2.1.2. Estações de trabalho, smartphones, tablets e notebooks distribuídos para os usuários (servidores e magistrados) que utilizam os serviços providos pela Secretaria de Tecnologia da Informação – SETIN-TJCE;

2.1.3. Os switches e roteadores compõem a infraestrutura lógica (tráfego de dados e acesso à internet) provendo o compartilhamento de recursos, conectando todos os dispositivos, inclusive computadores, impressoras e servidores. Tais dispositivos proporcionam o compartilhamento de informações sensíveis às atividades executadas pelo Judiciário Cearense. Portanto, torna-se impossível a concepção de uma rede lógica, sem a utilização dos mesmos.

2.1.4. Assim como um switch, o roteador conecta vários dispositivos para criar uma rede. Além disso, um roteador conecta vários switches e suas respectivas redes para formar uma rede ainda maior. Essas redes podem estar em um único local ou em vários;

2.1.5. Os servidores, alocados no Centro de Documentação e Informática – CDI – Prédio Anexo ao Palácio da Justiça, comportam quase todos os serviços e sistemas disponibilizados para o público externo e interno deste Tribunal;

2.1.6. É composta também, pela infraestrutura contida nas tabelas abaixo:

HOSTS DIFERENTES
Imagens de computadores
Imagens de notebooks
Switchs
Firewalls pequenos
Access Points - AP’s
Controladoras dos AP’s
Servidores físicos
Servidores diferentes – Windows 1
Servidores diferentes – Windows 2

Servidores diferentes – Windows 3
Servidores diferentes – Linux 1
Servidores diferentes – Linux 2
Servidores diferentes – Linux 3
Servidores diferentes – Linux 4
Servidores diferentes – Linux 5
Impressoras Multifuncionais
Balanceador de Carga – Netscaler
Firewall de grande porte – NGFW
Fitotecas – Tape Library
Switches de Núcleo
Servidores de Armazenamento – Storage
Relógio de Ponto
Controle de Acesso

Conteiners
Pje
IP3
MinIO
Pje Mídias
Portal SAJ
SAJ CAS
SAJ PG
SAJ SG
DJE - SAJ
SAJ CPOPG
SAJ AT
Openshift
AUTDOC - API
AUTDOC - Autenticação
PAJ
SAV
SCP - Sistema de Certidão de Precatórios
Aplicação de Referência (Ruby On Rails)
DJe - Administração
Dje - Consulta Pública

FATJ
FERIAS SERVIDOR
Gestão a Vista
INDICA
Manager ProTJ
Minha ESMEC
Novo SAA
Novo SCONC
SADJUS
SAE
SASR
SBIM
SCGV
SCI
SCN
SCT
SDTS
SEI
SGM
SIM TJ
SISNUGEP
SISPORT - Sistema de Controle de Portaria
SSAS-Sistema de Solicitação de Auxílio Saúde
TJCE Mobile Notifications API
Redmine
TJCE Mobile API
Discovery
Gateway
Keycloak
Redis
Rabbitmq
Awx
codex
codex pje pg
codex pje sg
pje binários

registry portal esaj
Vault portal esaj
Aplicações Java

Sites / Domínios
Total Geral (Origem Netscale - Disponibilizado na Internet)
Externos – Principais
Sites de aplicação judicial:
Malote Digital
Encurtador de link
tjcev2
Consulta processo (SCPU
E-saj
Pje
Sites administrativos:
Sites de admrh (portal)
Themis
Portal Adm (Ead)
Spes
ssas
Espaço do Servidor
webmail
Catinet (Versão externa)
CatiWeb (Versão externa)
Sasr
Processo Administrativo – CPA
VDC
Sites de aplicativos / sistemas
Sites de informações gerais

2.2. Descrição da Oportunidade ou do Problema

2.2.1. As funcionalidades dos equipamentos citados podem vir a sofrer degradação, tendo em vista o risco de invasão por parte de terceiros mal-intencionados, seja por meio de acesso a sites, por meio de aplicativos, ou e-mails que contém em seus anexos *malwares (software intencionalmente feito para causar danos a um computador, servidor, cliente, ou*

a uma rede de computadores) que podem comprometer a segurança de dados dos usuários que os utilizam.

2.2.2. O trabalho de manter a segurança de tais ativos, incluindo os de rede e de segurança, seguros vai além da utilização de antivírus nos computadores. Softwares desatualizados em estações de trabalho, notebooks e servidores, podem vir a criar alvos fáceis para exploradores de vulnerabilidades.

2.2.3. O intuito deste planejamento é abordar os principais tipos de vulnerabilidades – softwares maliciosos e ataques – demonstrando assim a importância e necessidade da aquisição de uma solução de análise de vulnerabilidade.

2.2.4. O intuito da utilização desse tipo de software é automatizar e facilitar a descoberta de vulnerabilidades em todos os ativos que estejam vinculados à rede do TJCE, para correção, antes que as mesmas sejam exploradas por atacantes e, neste contexto, é de grande importância seu adequado funcionamento.

2.3. Motivação da Demanda

2.3.1. Vulnerabilidade é um conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

2.3.2. Já segundo o CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.BR, uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

2.3.3. As vulnerabilidades são originadas de falhas na maioria das vezes não intencionais. Estas falhas podem ser:

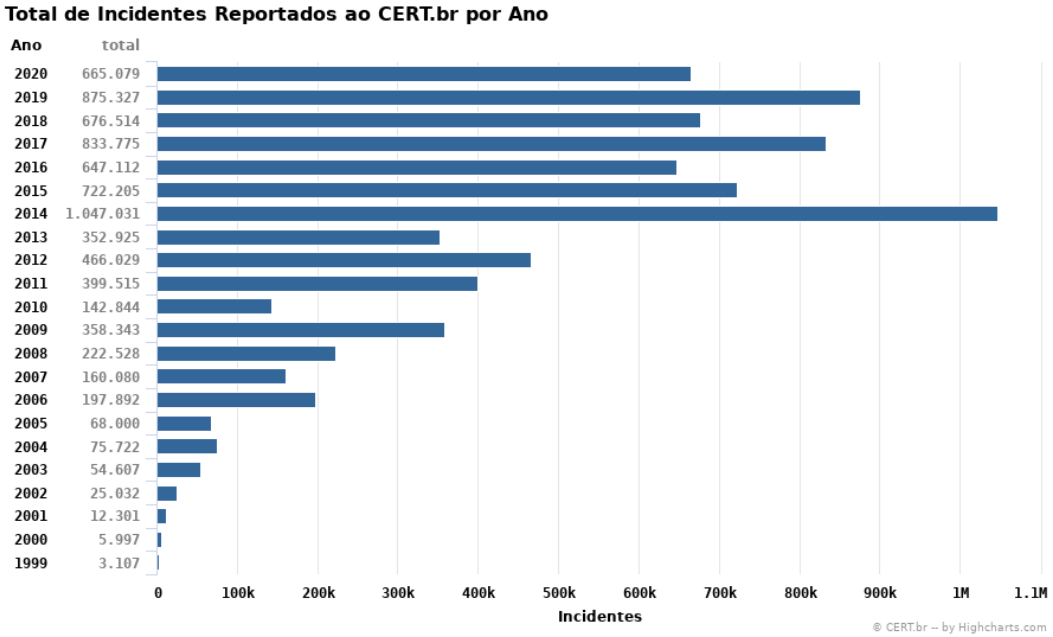
2.3.3.1. **Físicas:** Acesso a ativos por pessoas não autorizadas, devido à falta de controle de acesso. Por exemplo, uma empresa terceirizada de limpeza desligar um switch por engano.

2.3.3.2. **Hardware:** Falhas no Hardware que ocasionam indisponibilidade no sistema ou perda dados. Outro item desta falha é a inclusão de um hardware malicioso como um Keylogger.

2.3.3.3. **Naturais:** Desastres naturais comprometendo a segurança dos dados armazenados.

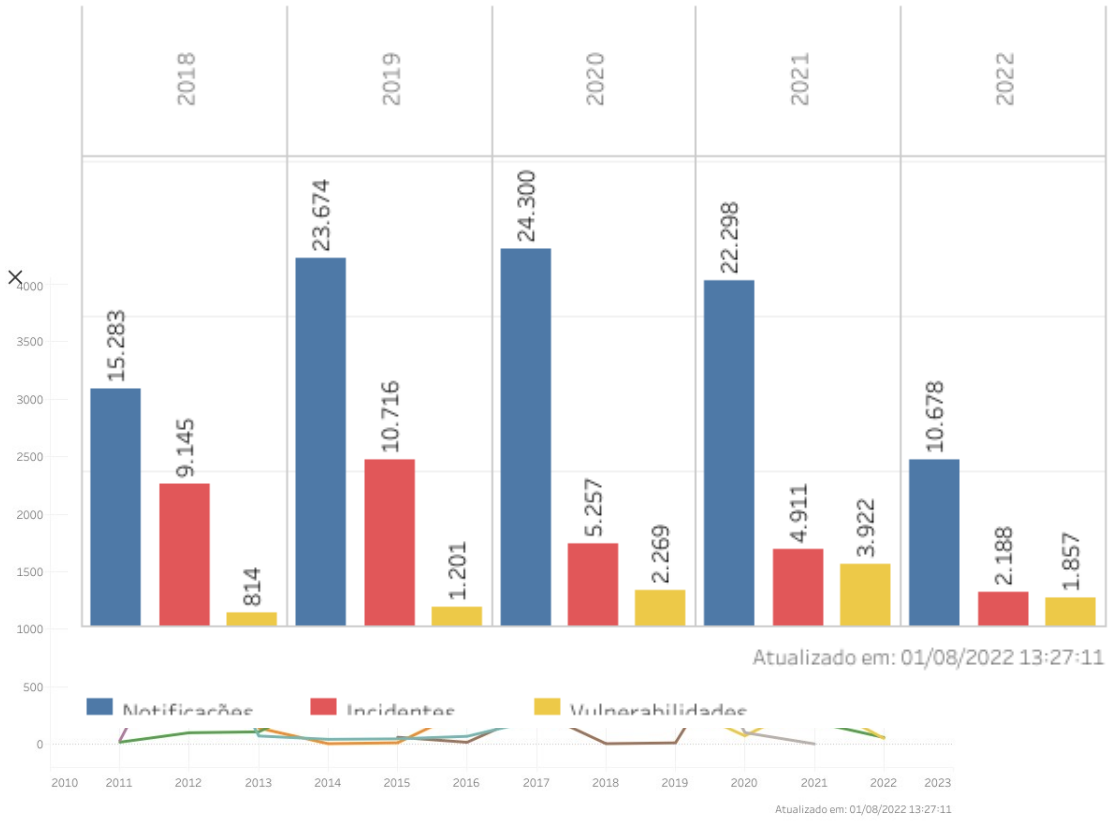
2.3.3.4. **Humanas:** Operador de sistema utilizar erroneamente uma função, prejudicando o funcionamento do mesmo ou ocasionando perda de informações.

2.3.3.5. **Software:** Falhas de programação, abrindo brechas a serem exploradas.

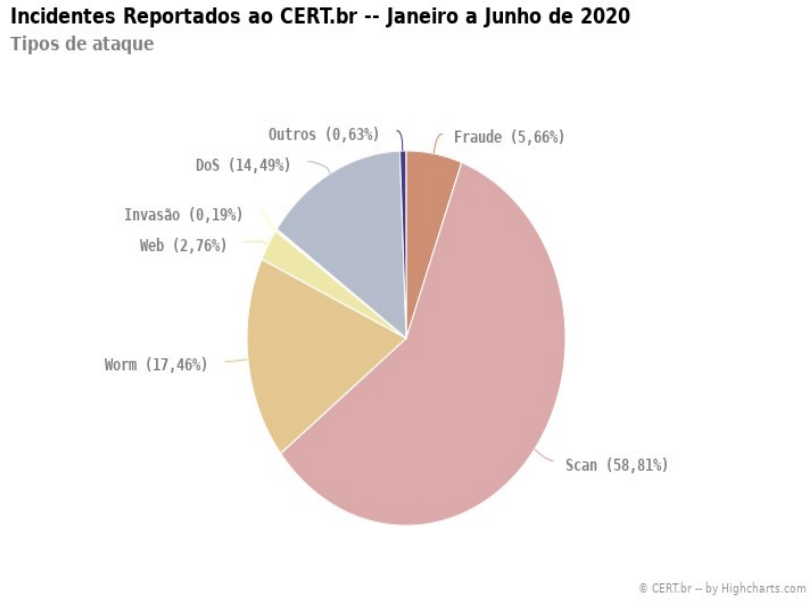


2.3.4. As estatísticas de incidentes do CERT.BR reportados de janeiro a junho de 2020, citadas na imagem acima, demonstram que 58,81% de incidentes são do tipo de ataque Scan, onde o atacante faz uma varredura de portas abertas em uma rede para identificar os serviços disponibilizados e suas possíveis vulnerabilidades.

2.3.5. Corroborando com as estatísticas apresentadas acima, podemos citar ainda os índices apurados pelo CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, cujas imagens abaixo indicam as ocorrências acerca de vulnerabilidades:



2.3.6. Muitas vulnerabilidades são exploradas ou criadas a partir de softwares desenvolvidos para este fim conhecidos como Malware. Proveniente do inglês malicious software o Malware é um programa que produz efeitos danosos e indesejados.



2.3.7. Os principais tipos de Malware encontrados hoje são:

2.3.7.1. **Vírus:** Programa capaz de se autoexecutar e infectar outros arquivos com seu próprio código.

2.3.7.2. **Worm:** Programa malicioso que se propaga sem a necessidade de infectar outros arquivos, diferentemente do vírus, sua propagação é feita sem intervenção humana utilizando vulnerabilidades em uma rede.

2.3.7.3. **Bot e botnet:** Bot é um programa que permite ser controlado remotamente para executar vários comandos maliciosos, como, por exemplo, ataque de negação de serviço a um site. Uma botnet é uma rede com vários bots no qual sua ação maliciosa

é amplificada.

2.3.7.4. Spyware: Os Spywares coletam informações pessoais ou empresariais e as enviam para terceiros. O Keylogger é um tipo de Spyware que captura as teclas digitadas pelo usuário, geralmente utilizado para roubar senhas.

2.3.7.5. Backdoor: O Backdoor ou Porta do fundo é uma vulnerabilidade que abre uma brecha para o atacante obter acesso indevido.

2.3.7.6. Cavalo de tróia: Também conhecido como Trojan o Cavalo de Tróia é um programa malicioso que se disfarça por um programa bem-intencionado. O usuário executa, sem saber, um código malicioso pensando que está executando apenas um programa legítimo. Eles geralmente são disseminados por e-mails e redes sociais se passando por cartões, álbum de fotos, jogos e etc.

2.3.7.7. Rootkit: Conjunto de programas utilizado por um atacante para ocultar sua invasão e facilitar um futuro ataque. Os Rootkits podem ser utilizados em outros malwares para dificultar a detecção destes.

2.3.8. A efetivação de um ataque é o êxito na exploração de uma ou mais vulnerabilidades. As motivações para realizar um ataque segundo o Cert.br, podem ser financeiras, por prestígio, demonstração de poder, por ideologia ou comerciais.

2.3.9. Com novas tecnologias novos ataques surgem, mas os principais ataques conhecidos atualmente são:

2.3.9.1. DoS e DDoS: Negação de Serviço do inglês Denial of Service, sigla DoS, ocorre quando um site (ou serviço) fica indisponível por receber uma grande quantidade de tráfego, não podendo atender as requisições legítimas. Os ataques DDoS (Distributed Denial of Service) são vários ataques DoS feitos de maneira distribuída dificultando assim o bloqueio da origem os ataques. Geralmente estes ataques provêm de computadores infectados com Bots participantes de uma rede Botnet.

2.3.9.2. Buffer Overflow: ou Estouro de Buffer ocorre quando um espaço de memória com tamanho fixo recebe um dado maior que seu tamanho, ocorrendo assim um vazamento dados na memória sobrescrevendo a memória adjacente.

2.3.9.3. Spam: são e-mails não solicitados que são enviados em massa gerando tráfego desnecessário nas redes. Geralmente os Spams têm como intuito a divulgação de produtos, mas também são responsáveis por muitos golpes de Internet por disseminarem Malwares.

2.3.9.4. Phishing Scam: E-mails falsos que se passam por mensagens de instituições confiáveis, como bancos e órgãos governamentais. Seu intuito é induzir o usuário a instalar um programa malicioso ou visitar uma página falsa (cópia de uma

verdadeira) para obter dados pessoais, como por exemplo, senhas e números de cartão de crédito. Segundo o Cert.br 87,05% das fraudes de janeiro a dezembro de 2019 eram de páginas falsas, conforme apresentado na imagem acima.

2.3.10. Tipos de incidentes de segurança da informação:

2.3.10.1. DNS Poisoning: Envenenamento de DNS é um ataque que forja um endereço falso no servidor de DNS. Assim, o atacante pode capturar senhas e números de cartões de crédito utilizando páginas clones do site original.

2.3.10.2. Ataque de Força Bruta: Programa que utiliza várias combinações de usuário e senha para conseguir acesso indevido a sistemas ou para descriptografar chaves e arquivos. Além do risco de acesso indevido, o Ataque de Força Bruta gera uma carga excessiva no alvo por ter responder e processar a várias tentativas de logins. Esta técnica é muito utilizada em servidores de SSH mal configurados.

2.3.10.3. Packet Sniffing: Packet Sniffing ou Farejamento de Pacotes é um método utilizado para capturar pacotes destinados a outras máquinas da mesma rede com objetivo de obter dados pessoais. Ativos de rede que utilizam broadcast de pacotes, como Hub, facilitam o farejamento dos pacotes. Em redes segmentadas por Switches o Packet Sniffing é possível com a utilização de outra técnica conhecida como Man-in-theMiddle (MiTM). Com MiTM o atacante forja a passagem dos pacotes da rede pela sua interface através do envenenamento da tabela ARP dos outros computadores.

2.3.10.4. Varreduras em Redes – Scan: Técnica onde o atacante descobre máquinas ativas e serviços disponíveis na rede. Em uma rede 192.1 68.0.0/24, por exemplo, o atacante envia ping para todos endereços possíveis para descobrir quais estão ativos. Com os endereços das máquinas ativas é feita uma nova varredura em cada máquina para descobrir suas portas abertas e seus respectivos serviços. Com isso o atacante pode explorar as vulnerabilidades destes serviços e prejudicar o computador alvo. Por exemplo, sabendo que o alvo possui a porta TCP 23 aberta, o atacante irá explorar vulnerabilidades de software ou configuração do serviço para obter acesso ao sistema.

2.3.10.5. SQL Injection: O ataque de Injeção de SQL consiste em inserir códigos SQL em um software vulnerável para obter ou danificar informações do Banco de dados.

2.3.10.6. CSS – Cross Site Scripting: XSS ou CSS o Cross Site Scripting é um ataque a um site vulnerável que aceita a inserção de códigos Javascript. Através do CSS o atacante pode inserir uma página externa para capturar logins e senhas.

2.4. Resultados Pretendidos

2.4.1. **Maior controle de segurança da informação e proteção de dados no âmbito do TJCE**: através da redução de *malwares*, sistemas desatualizados, dentre outros problemas;

2.4.2. **Aumento dos esforços de correção e testes de eficácia:** as análises de vulnerabilidades de rede permitem não só a identificação de problemas de rede, mas também ajuda na sua priorização e no desenvolvimento de uma estratégia para lidar com aqueles mais críticos;

2.4.3. **Melhoria na gestão de mudanças e no gerenciamento de patches**: faz parte da gestão de vulnerabilidades centralizar e gerar todos os feedbacks sobre os problemas, as suas correções e as próximas ações;

2.4.4. **Fortalecimento da atuação das equipes que gerem soluções críticas**: A identificação e o tratamento das vulnerabilidades auxiliarão a SETIN na execução de suas responsabilidades de análise e respostas às notificações e atividades relacionadas a incidentes de segurança em redes de computadores além da redução desses incidentes;

2.4.5. **Apoio nas auditorias de Segurança da Informação e Comunicações**: a obtenção de relatórios detalhados permitirá a devida diligência durante as auditorias;

2.4.6. **Atualização da Política de Segurança da Informação e Comunicações**: O gerenciamento de vulnerabilidades possibilitará aplicar melhorias na segurança da informação e na revisão da Política de Segurança da Informação e Comunicações e suas normas complementares;

2.4.7. **Auxílio nos requisitos regulamentares**: A identificação e o tratamento das vulnerabilidades contribuirá para que o TJCE se mantenha em conformidade com:

2.4.7.1. Resoluções, Normativos e Portarias editados pelo Conselho Nacional de Justiça – CNJ;

2.4.7.2. Os princípios e controles de segurança definidos nos padrões ABNT NBR ISO/IEC 27001, 27002, 27005, 27011 e 27014;

2.4.7.3. A Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

2.4.7.4. Os frameworks de processos de governança e boas práticas como o ITIL e COBIT.

2.4.8. Não obstantes os aspectos técnicos citados anteriormente, que por sua venham a impingir a Administração a ponderar acerca da implantação da referida solução, é oportuno citar que o CNJ, Órgão cuja competência é o de o controlar da atuação administrativa e financeira do Poder Judiciário (Regimento Interno Nº 67 de 03/03/2009), vinculando assim as diretrizes do TJCE quanto às soluções de TI, editou a Portaria Nº 162 de 10/06/2021, A*prova protocolos e Manuais criados pela Resolução CNJ nº. 396/2021, que*

institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)., cujos enunciados e ANEXOS instruem:

Protocolo – Prevenção de Incidentes Cibernéticos do Poder Judiciário – PPINC-PJ

4.1 A gestão de incidentes de segurança cibernética é realizada por meio de processo definido e constituída formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

5.3 Caberá a cada órgão do Poder Judiciário avaliar o adequado posicionamento da ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética) em seu organograma institucional, considerando-se seu desenho organizacional e suas peculiaridades.

2.4.9. Para a efetivação da implantação, atualização e acompanhamento da política de segurança, almejada pela solução em questão, faz-se necessária a inclusão de treinamentos e consultoria, tendo em vista o atendimento do requisito de independência do conhecimento.

ANEXO IV DA PORTARIA No 162, DE 10 DE JUNHO DE 2021

Manual de Referência – Proteção de Infraestruturas Críticas de TIC

Checklist para utilização dos Controles Mínimos Recomendados

Gerenciamento Contínuo de Vulnerabilidade		
3.1	Utilizar uma ferramenta atualizada e compatível com o SCAP para efetuar varreduras automatizadas em todos os ativos conectados à rede com frequência semanal ou inferior. para identificar todas as vulnerabilidades potenciais nos sistemas da organização.	Detectar
3.2	Realizar varreduras por vulnerabilidades com contas autenticadas em agentes executados localmente em cada sistema, ou varreduras por *scanners* remotos que sejam configurados com privilégios elevados nos sistemas que estejam sendo testados.	Detectar
3.3	Utilizar uma conta dedicada para as varreduras por vulnerabilidades autenticadas, que não deve ser utilizada para quaisquer outras atividades administrativas e que deve ser vinculada a equipamentos específicos, em endereços IP específicos.	Detectar
3.4	Implantar ferramentas de atualização automatizada de *software*, de forma a garantir que os sistemas operacionais sejam executados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	Proteger
	Implantar ferramentas de atualização automatizada de *software* de forma	

3.5	a garantir que os *softwares* de terceiros em todos os equipamentos sejam utilizados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	Proteger
3.6	Utilizar um processo de classificação de riscos para priorizar a remediação de vulnerabilidades descobertas.	Respon der

2.5. Levantamento das alternativas

2.5.1. O Estudo Técnico Preliminar identificou três soluções possíveis para o Gerenciamento de Vulnerabilidades:

2.5.1.1. Cenário 1

Solução	Utilização de solução do Portal do Software Público Brasileiro
Descrição	O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e é compartilhado sem ônus no Portal do Software Público Brasileiro, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade.
Fornecedor	Portal do Software Público Brasileiro
Análise da Solução	O presente cenário tem o objetivo de analisar a adquisição junto ao Portal do Software Público Brasileiro para atender às necessidades do TJCE. O principal objetivo do Portal é promover o desenvolvimento de um ambiente colaborativo que não só reduz os custos do governo, mas também permite o desenvolvimento de artefatos tecnológicos. A rede estabelecida cria um complexo sistema de garantias econômicas, políticas e relações sociais que envolvem diversas esferas da sociedade. O software, neste contexto, não é apenas um produto, mas também um artefato, por meio do qual, seus criadores proporcionam novos referenciais de produção. Conforme pesquisa no portal de software público Brasileiro, constam softwares disponíveis no portal, no entanto não se encontra disponível nenhuma solução de gestão de vulnerabilidades. Conclui-se pelos fatos expostos que não é possível adotar os softwares disponíveis no Portal de Software Público Brasileiro para atender às necessidades do TJCE.

2.5.1.2. Cenário 2

Solução	Utilização de softwares livres
Descrição	Utilização de ferramentas livres ou gratuitas, como os softwares Wireshark, Nmap, Metasploit, OpenVas.
Fornecedor	Comunidades Open Source
Análise da Solução	A solução proposta atende apenas parte da necessidade, pois a utilização desse cenário implica não contar com suporte técnico especializado, ademais a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos. Além disso, a adoção da solução proposta, por não possuir uma equipe dedicada de

	pesquisadores para avaliar e atualizar a ferramenta quando da descoberta de vulnerabilidades de dia zero não provê uma atualização tempestiva, não atendendo às necessidades do TJCE. A vulnerabilidade de dia zero é uma vulnerabilidade encontrada em um sistema, um hardware ou um software e pode ser uma porta para ameaças, como um ataque de malware. Em outras palavras, vulnerabilidade de dia zero é uma falha que precisa ser corrigida o mais rápido possível por causa dos riscos que ela gera para as organizações. Ela pode ocasionar uma exploração de dia zero, um ataque digital que faz uso das vulnerabilidades de dia zero para instalar softwares maliciosos em um dispositivo. Outro ponto desfavorável ao cenário apresentado é que os relatórios fornecidos pelas ferramentas não apresentariam rastreabilidade das atividades já realizadas nos ativos e sistemas, pois seriam utilizadas ferramentas de diferentes fabricantes para realização de diferentes atividades complementares. Seriam utilizadas, por exemplo, ferramentas específicas para detectar dispositivos remotos, como firewalls e roteadores com suas marcas e modelos, além da verificação de conexões e pacotes de rede como é o caso do Nmap e Wireshark. Outras ferramentas como o Metasploit e OpenVas para realizar exames rigorosos contra um conjunto de endereços IP e outras ferramentas de scanners para segurança de rede sem fio como Aircrack. Assim, como se vê a solução proposta não atende grande parte das necessidades tecnológicas e de negócio requeridas pelo Ministério.

2.5.1.3. Cenário 3

Solução	Contratação de empresa especializada para fornecimento e instalação de solução de gestão e análise de vulnerabilidades de ativos, por meio do fornecimento e instalação de solução de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de Consultoria Especializada, suporte, com garantia (manutenção e suporte técnico).
Descrição	Aquisição de software de gerenciamento de vulnerabilidades em Ativos e web applications, com modelo de licenciamento anual
Fornecedor	Brinqa, Digital Defense, Expanse, Kenna Security, NopSec, Outpost24, Qualys, Rapid7, RedSeal, RiskIQ, RiskSense, Skybox Security e Tenable
Entidade	**MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA – ATA DE REGISTRO DE PREÇOS Nº 11/2021;** **TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO – ATA DE REGISTRO DE PREÇOS Nº 005/2022;**
Análise da Solução	Nesse cenário é contemplado a aquisição de solução baseada em nuvem (cloud computing). Essa solução apresenta facilidade de gerenciamento, valor de aquisição adequado e atualização automática da plataforma. No modelo de contratação em nuvem, todo o faturamento será na forma de custeio. Todas os requisitos de funcionalidades do projeto são atendidos por esse cenário. As soluções analisadas Qualys (VM e WAS) e Tenable.io conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Ambas foram testadas com versão de avaliação e os resultados e relatórios se mostraram adequados.

2.5.2. SOLUÇÕES PAGAS DISPONÍVEIS NO MERCADO

2.5.2.1. F-Secure Elements Vulnerability Management.

2.5.2.1.1. Descrição do fabricante: O F-Secure Elements Vulnerability Management faz parte do F-Secure Elements, a única plataforma que oferece tudo, desde gerenciamento de vulnerabilidade e proteção de colaboração até proteção de endpoint; e detecção e resposta – gerenciadas a partir de um único console de segurança. Use soluções individuais para necessidades específicas ou obtenha proteção completa combinando todas elas.

2.5.2.2. Qualys Vulnerability Management.

2.5.2.2.1. Descrição do fabricante: A solução mais avançada, escalonável e extensível da indústria para gerenciamento de vulnerabilidade. Baseado em nuvem, o Qualys VM oferece visibilidade global de onde seus ativos de TI são vulneráveis e como protegê-los, com: Detecção baseada em agente, Monitoramento e alertas constantes e Cobertura e visibilidade abrangentes.

2.5.2.3. Rapid7 InsightVM.

2.5.2.3.1. Descrição do fabricante: A plataforma Rapid7 Insight, lançada em 2015, reúne a biblioteca Rapid7 de pesquisa de vulnerabilidade, conhecimento de exploração, comportamento global de invasores, dados de varredura em toda a Internet, análise de exposição e relatórios em tempo real para fornecer uma maneira totalmente disponível, escalonável e eficiente de coleta de dados de vulnerabilidades para tomada de decisão.

2.6. Alinhamento estratégico

ID	Objetivo Estratégico Institucional	ID	Objetivos de Contribuição da Setin
01	Fortalecer a inteligência de dados e a segurança da informação	01	Proporcionar segurança, disponibilidade e confiabilidade às informações dos sistemas, plataformas e ferramentas institucionais

2.6.1. A contratação de **Solução de gestão e análise de vulnerabilidades de ativos**, está alinhada e presente no mapa do Planejamento Estratégico do TJCE 2030 com os objetivos de:

2.6.1.1. FORTALECER A INTELIGÊNCIA DE DADOS E A SEGURANÇA DA INFORMAÇÃO.

2.6.1.2. ANEXO II – INDICADORES E METAS DESDOBRAMENTO DA ESTRATÉGIA – SETIN

2.6.1.2.1. Indicador 1: Índice de Serviços Críticos com Gestão de Risco.

2.6.1.2.1.1. Fortalecer a inteligência de dados e a segurança da informação.

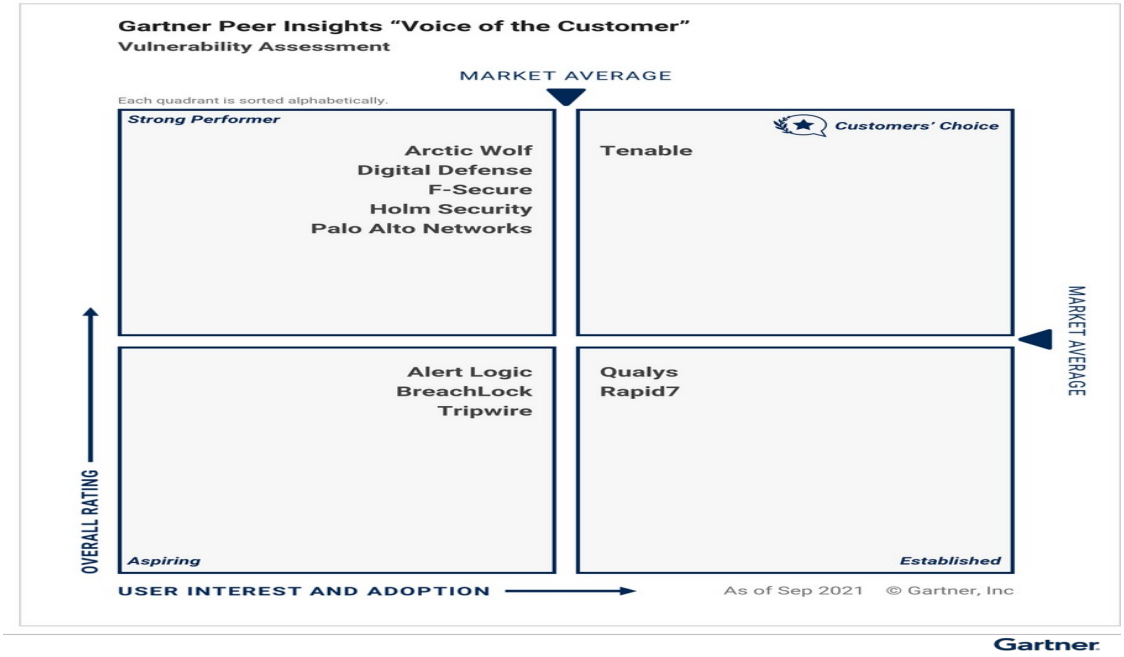
2.6.1.2.2. Indicador 2: Índice de conformidade com as políticas de segurança de TIC.

2.7. Critérios Ambientais

2.7.1. Promover a correta destinação dos resíduos resultantes da prestação do serviço, tais como peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental como a Política Nacional de Resíduos Sólidos (Lei no 12.305/2010).

2.8. Justificativa da Solução Escolhida

2.8.1. Com base no estudo, que levou em consideração o quadrante apresentado abaixo, foram priorizadas as soluções com posição de destaque (leaders) que possuam as principais funcionalidades de soluções de Gerenciamento de Vulnerabilidades para atender às necessidades da demanda elencada no Documento de Oficialização da Demanda – DOD.



2.8.2. O objetivo do estudo é avaliar os benefícios na adoção de uma solução específica, observando os critérios de eficácia, eficiência, economicidade e padronização, bem como subsidiar a elaboração dos demais artefatos presentes na resolução CNJ no 182/2013, como a sustentação do contrato, a estratégia da contratação, a análise de risco e, por fim, o Termo de Referência;

2.8.2.1. A análise das soluções levou em consideração:

2.8.2.1.1. As alternativas do mercado;

2.8.2.1.2. A existência de software público brasileiro;

2.8.2.1.3. As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

2.8.2.1.4. As necessidades de adequação do ambiente do TJCE para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado

para prestação do serviço, etc);

2.8.2.1.5. A possibilidade de aquisição na forma de bens ou contratação como serviço;

2.8.2.1.6. Os diferentes modelos de prestação do serviço;

2.8.2.1.7. Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

2.8.3. TECNOLOGIA TENABLE

EMPRESA – A				
ITEM	**ESPECIFICAÇÃO**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	150	R$ 1.538,65	R$ 230.797,50
2	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	114	R$ 1.783,90	R$ 203.364,60
3	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	400	R$ 1.912,22	R$ 764.888,00
4	Suporte Técnico Especializado	24	R$ 13.479,85	R$ 323.516,40
5	Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.	8	R$ 9.526,30	R$ 76.210,40
			VALOR GLOBAL	**R$ 1.598.776,90**

EMPRESA – B				
ITEM	**ESPECIFICAÇÃO**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	150	R$ 2.033,00	R$ 304.950,00
2	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	114	R$ 2.210,00	R$ 251.940,00
3	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	400	R$ 1.867,00	R$ 746.800,00

4	Suporte Técnico Especializado	24	R$ 19.000,00	R$ 456.000,00
5	Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.	8	R$ 12.000,00	R$ 96.000,00
			VALOR GLOBAL	**R$ 1.855.690,00**

EMPRESA – C				
ITEM	**ESPECIFICAÇÃO**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	150	R$ 1.333,12	R$ 199.968,00
2	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	114	R$ 1.378,00	R$ 157.092,00
3	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	400	R$ 1.831,00	R$ 732.400,00
4	Suporte Técnico Especializado	24	R$ 19.000,00	R$ 456.000,00
5	Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.	8	R$ 14.000,00	R$ 112.000,00
			VALOR GLOBAL	**R$ 1.657.460,00**

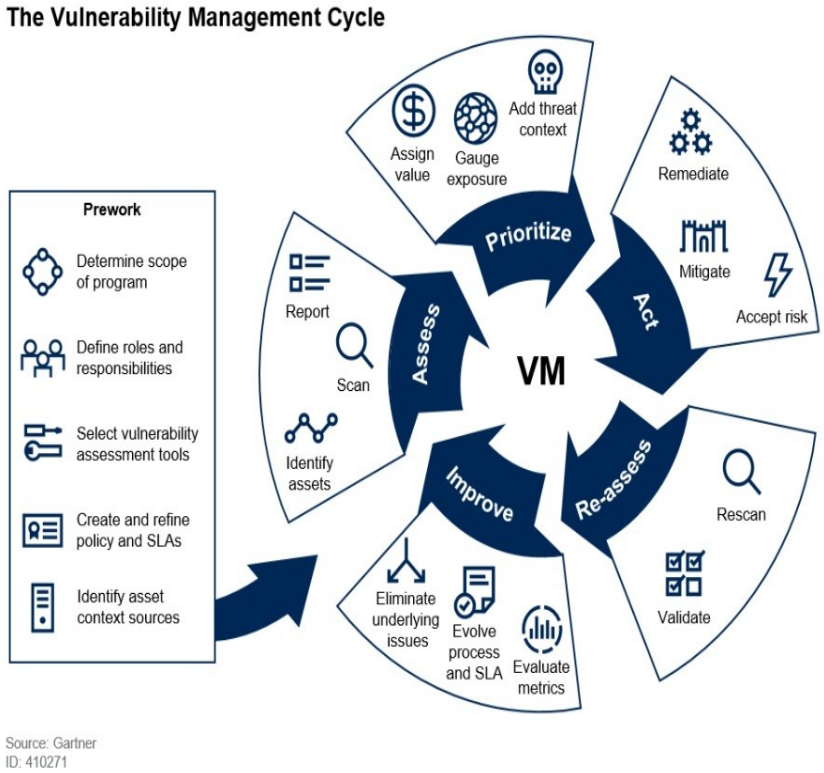
VALORES MÉDIOS – TECNOLOGIA TENABLE				
ITEM	**ESPECIFICAÇÃO**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	150	R$ 1.634,92	R$ 245.238,00
2	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	114	R$ 1.790,63	R$ 204.131,82
3	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	400	R$ 1.870,07	R$ 748.028,00
4	Suporte Técnico Especializado	24	R$ 17.159,95	R$ 411.838,80
5	Treinamento técnico da Solução de Gerenciamento de vulnerabilidades.	8	R$ 11.842,10	R$ 94.736,80
			VALOR GLOBAL	**R$ 1.703.973,42**

Vale ressaltar que a comparação de mercadológica entre ferramentas de diferentes fornecedores indicados no

Cenário 3 restou prejudicada. A SETIN entrou em contato com fornecedores da solução Rapid7 através de e-mail e demais meios, não logrando êxito no retorno dos mesmos e comprometendo a análise de outras soluções privadas.

2.8.4. Preliminarmente, observa-se que embora outras soluções de mercado demonstrem-se viáveis e comercialmente competitivas, convém explicitar aspectos tecnológicos triviais, frutos de análises mais aprofundadas, com o intento de demonstrar não apenas as vantagens pecuniárias que podem ser obtidas, mas, de forma significativa, a avaliação dos riscos, e por conseguinte, prejuízos gravosos que a Administração estaria sujeita, caso não ponderasse a atuação de outras soluções de vulnerabilidade. Por meio deste estudo, pode-se concluir que o mercado de soluções de vulnerabilidade é variado, embora seja imperativo citar que a avaliação das soluções disponíveis no mercado foram balizadas de forma a criar um ambiente tecnológico que provisione integralmente os recursos ora descritos na tabela presente nos itens **2.5 e 4.2.1**.

2.8.5. No entanto, a escolha de uma ferramenta de avaliação de vulnerabilidades em pleno funcionamento é um pré-requisito extraído, extraída do site https://blogs.gartner.com/augusto-barros/2019/10/25/new-vulnerability-management-guidance-framework/, conforme na imagem abaixo:



2.8.6. Com base neste levantamento, os cenários descritos no item **2.5** apontam as soluções possíveis para atendimento da necessidade;

2.8.7. Conforme indicado no item **2.5**, os **cenários 1 e 2** se mostram insuficientes para o

atendimento da demanda do TJCE de forma plena.

2.8.8. CENÁRIO 1 – Solução Utilização de solução do Portal do Software Público Brasileiro.

2.8.8.1. Não existe solução disponível no Portal do Software Público Brasileiro.

2.8.9. CENÁRIO 2 – Utilização de softwares livres.

2.8.9.1. A solução proposta 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.

2.8.9.2. É oportuno citar que a SETIN-TJCE, no decorrer do processo de identificação de soluções viáveis para atender a demanda proposta pelo planejamento, identificou a celebração da Ata de Registro de Preços 005/2022 entre a empresa IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA EIRELI e o Tribunal Regional do Trabalho da 8ª Região, cujos valores adjudicados demonstram vantajosidade, face aos valores propostos por outras empresas que compõem a média de preços, conforme demonstrados no item **7**. Ao passo que, em observância ao princípio da economicidade, indica-se que a contratação da solução proposta deverá ocorrer mediante adesão à referida ARP.

2.9. Justificativa para Parcelamento do Objeto

2.9.1. A contratação constitui objeto organizado em lote único, não se aplicando o parcelamento. Embora considerando o aspecto da economicidade pelo fato da participação de vários fornecedores, caso houvesse a divisão por lotes, a presente contratação deverá é balizada tanto em parâmetros mercadológicos – fornecedores da solução habilitados pelo fabricante dispõem de todas as ferramentas que compõem o objeto - bem como devido ao fato da unicidade tecnológica a qual a solução deve obedecer.

2.10. Natureza do Objeto

2.10.1. Verifica-se que os Serviços Integrados para Solução de gestão e análise de vulnerabilidades de ativos e aplicações web do TJCE, são oferecidos por diversos fornecedores no mercado de TIC e apresentam características padronizadas e usuais. Assim, pode-se concluir que o objeto é comum, nos termos da Lei Federal N° 10.520/2002, e, portanto, como melhor opção, a utilização da modalidade “Pregão” sendo, preferencialmente, em sua forma eletrônica e do tipo “Menor Preço”;

2.11. Natureza do Serviço, se Continuado ou não

2.11.1. Verifica-se também que os serviços que compõem a solução constituem demanda de caráter contínuo, uma vez que está vinculada ao atendimento das necessidades que se apresentam rotineiramente para a automatização e melhoria de processos de trabalho do TJCE. Portanto, a necessidade de o TJCE dispor de Serviços Integrados para Solução de Colaboração renova a cada ano, o que remete ao entendimento de caracterização de prestação continuada;

2.12. Justificativa para Adoção do Pregão

2.12.1. A adoção do Pregão Eletrônico, de acordo com o disposto no Decreto Nº 10.024, de 20 de Setembro De 2019, destina-se à aquisição de bens e serviços comuns, no âmbito da União, e submete-se ao regulamento estabelecido neste Decreto.

2.12.2. O pregão, na forma eletrônica, como modalidade de licitação do tipo menor preço, realizar-se-á quando a disputa pelo fornecimento de bens ou serviços comuns for feita à distância em sessão pública, por meio de sistema que promova a comunicação pela internet.

[...]

Art. 1º Este Decreto regulamenta a licitação, na modalidade de pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.

§ 3º Para a aquisição de bens e a contratação de serviços comuns pelos entes federativos, com a utilização de recursos da União decorrentes de transferências voluntárias, tais como convênios e contratos de repasse, a utilização da modalidade de pregão, na forma eletrônica, ou da dispensa eletrônica será obrigatória, exceto nos casos em que a lei ou a regulamentação específica que dispuser sobre a modalidade de transferência discipline de forma diversa as contratações com os recursos do repasse.

2.13. Justificativa para Aplicação do Direito de Preferência (Lei complementar nº 123/06 e Lei nº 8.248/91)

2.13.1. Não incide sobre a presente contratação, a aplicação do Direito de Preferência de que trata o

referido item.

2.14. Da Subcontratação, Cisão ou Incorporação

2.14.1. Não será permitida a subcontratação total ou parcial do objeto.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. Contratação de empresa especializada em serviços de tecnologia da informação e comunicação, para fornecimento e instalação de solução de gestão e análise de vulnerabilidades de ativos e aplicações web do TJCE, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado, conforme condições, quantidades e exigências estabelecidas neste documento e seus anexos.

4. ESPECIFICAÇÃO TÉCNICA

4.1. As especificações dos itens estão dispostas no ANEXO I – ESPECIFICAÇÕES TÉCNICAS deste documento.

4.2. Requisitos da Solução

4.2.1. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

4.2.1.1. Depreendendo-se do DOD (Documento de Oficialização da Demanda), elaborado conjuntamente pela área requisitante e para atender as necessidades da referida área, concomitante à análise específica do ambiente tecnológico do TJCE, faz-se imprescindível o atendimento as necessidades de negócio apresentadas nas tabelas que seguem:

ID	Funcionalidades
1	Aumento da segurança da informação e comunicação e o sigilo das informações do cidadão; Gerenciamento de Vulnerabilidades em ativos e Sistemas Operacionais; Gerenciamento de Vulnerabilidades em Sistemas e páginas WEB; Detecção e Correção de falhas de softwares que possam acarretar riscos na segurança, na funcionalidade e no desempenho dos sistemas; Implantação de mecanismos para realizar o bloqueio de ataques constantes; Foco na melhoria constante do sistema de segurança de dados corporativos; Auxílio na implementação de políticas de segurança; Agilidade na identificação de falhas.
ID	**Necessidades Tecnológicas**
1	Fornecimento de solução de segurança para proteção de aplicações, servidores físicos, virtuais e container com serviços de implementação e capacitação; Solução de análise de vulnerabilidades e Serviços técnicos especializados na área de Segurança da Informação; Análise de Vulnerabilidades; Gerenciamento de patches; Gerenciamento da configuração de segurança;

	Auditoria de software de alto risco; Detecção e mitigação de vulnerabilidades de dia zero; Aprimoramento da segurança dos servidores web.
ID	**Demais necessidades**
1	Integração e Customização dos Sistemas de Informação existentes; Otimização dos processos de infraestrutura da TIC conforme as melhores práticas; Testar os hosts (físicos e virtuais), comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por de software; Testar as aplicações e páginas web, internas e externas, comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurançapor grandes fabricantes de software; Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas. Aumento da proteção dos ativos de informação do Ministério da Justiça e Segurança Pública

4.3. Demais Requisitos

4.3.1. Seguem definidos no ANEXO I os requisitos atinentes à:

4.3.1.1. Capacitação;

4.3.1.2. Suporte Técnico Especializado/Manutenção.

<table>
<tr><td>Requisitos legais</td><td>Este ETP foi elaborado de acordo com o Ordenamento Jurídico Nacional que regulamenta o processo de aquisições para a Administração Pública;
Lei n. 8.666 de 21 de junho de 1993, Lei n. 10.520 de 17 de julho de 2002 e o Decreto n. 5.450, de 31 de maio de 2005, e constitui peça integrante, indispensável e inseparável do processo licitatório, visando viabilizar a aquisição dos bens e serviços descritos neste ETPC e seus Apêndices;
Resolução Nº 182 de 17/10/2013/Resolução Nº 326 de 26/06/2020, 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);
Os bens e serviços que constituem o objeto deste ETP enquadram-se no conceito de comuns, nos termos da Lei 10.520/02, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado;</td></tr>
<tr><td>Requisitos temporais:</td><td>Para a solução, deverá ser considerado o cronograma de eventos e prazos abaixo apresentado para a implantação da Solução. Os prazos apresentados são considerados como máximos, não impedindo, pois, que sejam cumpridos em prazos menores:
<table><tr><th>ID</th><th>EVENTO</th><th>RESPONSÁVEL</th><th>PRAZO</th></tr><tr><td>1</td><td>Assinatura do Contrato.</td><td>CONTRATANTE e CONTRATADA</td><td>Até 5 (cinco) dias após a convocação pelo CONTRATANTE.</td></tr><tr><td>2</td><td>Entrega de todos os componentes</td><td>CONTRATADA</td><td>Até 30 (trinta) dias após o evento 1.</td></tr></table></td></tr>
</table>

		da Solução.		
	3	Conferência dos componentes da solução.	CONTRATANTE	Até 05 (cinco) dias após o evento 2.
	4	Entrega do Plano de Implantação.	CONTRATADA	Até 10 (dez) dias após o evento 1.
	5	Aceite do Plano de Implantação.	CONTRATANTE	Até 05 (cinco) dias após o evento 4.
	6	Implantação da Solução – Homologação. *	CONTRATADA	Até 10 (dez) dias úteis após o evento 3.
	7	Implantação da Solução – Planejamento. *	CONTRATADA	Até 05 (cinco) dias úteis após o evento 6.
	8	Operação Assistida.*	CONTRATANTE e CONTRATADA	Até 05 (cinco) dias úteis após o evento 7.
	9	Emissão do Termo de Recebimento Definitivo – AQSETIN2022015 – ANEXO III – TRD	CONTRATADA	Até 5 (cinco) dias úteis após o evento 8.
	Demais requisitos temporais seguem estabelecidos no **ANEXO I**.			
Requisitos de Segurança	**Quanto a esfera administrativa/contratual a Empresa Fornecedora deverá observar os requisitos que seguem:** • A empresa fornecedora da solução de TI deverá tratar como "confidenciais" quaisquer informações, a que tenha acesso para execução do objeto, não podendo revelá-las ou facilitar sua disponibilização a terceiros. A obrigação permanecerá válida durante o período de vigência contratual e o seu descumprimento implicará em sanções administrativas e judiciais contra a empresa ofertante da solução de TI; • As obrigações e conhecimentos sobre os requisitos de segurança serão ratificados pelo TJCE e a empresa fornecedora da solução de TI através do Termo de Compromisso – ANEXO VI, com declaração de manutenção de sigilo e respeito às normas de segurança vigentes do TJCE em razão do trabalho vinculado ao contrato assinado. Pela mesma razão a licitante deverá providenciar o Termo de Ciência (ANEXO V) da Declaração de Manutenção de Sigilo e respeito às normas vigentes no órgão			

	ou entidade, a ser assinado por todos os empregados da licitante diretamente envolvidos na contratação. **Quanto ao cerne das funcionalidades do objeto, são almejados como requisitos:** • Gerenciamento de ameaças, como filtragem de mensagens e anti-malware; • Gerenciamento de dispositivo móvel, funcionalidade que permite criar e gerenciar políticas de segurança de dispositivos, limpar remotamente um dispositivo e exibir relatórios detalhados de dispositivos no tocante ao uso da aplicação; **Demais requisitos implícitos à segurança da solução estarão disponíveis em anexo próprio**
Requisitos sociais, ambientais e culturais:	A CONTRATADA deve estar habilitada juridicamente (art. 28 da Lei no 8.666/93) e em regularidade fiscal e trabalhista (art. 29 da Lei no 8.666/93). A CONTRATADA deve cumprir o disposto no inciso XXXIII do art. 7o da Constituição Federal de 1988, quanto ao emprego de menores. Promover a correta destinação dos resíduos resultantes da prestação do serviço, tais como peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental como a Política Nacional de Resíduos Sólidos (Lei no 12.305/2010). A documentação técnica e os manuais necessários à operação das ferramentas que compõem a solução devem ser disponibilizados, de preferência em idioma Português Brasileiro. Caso esse esteja indisponível, será aceito o idioma Inglês.

5. MODELO DE PRESTAÇÃO DE SERVIÇO / FORNECIMENTO DE BENS

5.1. Metodologia de Trabalho

5.1.1. Os serviços serão demandados de forma gradual e seu quantitativo poderá variar em virtude da flutuação natural demanda durante a execução contratual, portanto os quantitativos de licenças de software contratados representam meramente uma estimativa de utilização dos serviços. Não haverá nenhuma obrigação do TJCE na utilização do quantitativo total de licenças. Somente serão devidos e pagos os serviços efetivamente prestados, demandados através das respectivas Ordens de Serviço;

5.1.2. O prazo máximo para a efetivação das licenças é de até 20 (vinte) dias consecutivos, acrescentados do prazo de 7 (sete) dias úteis para a entrega da amostra prévia para verificação de conformidade do objeto, contados da emissão da Nota de Empenho;

5.1.3. O prazo máximo para a entrega de amostra prévia dos itens constantes na Ordem de Serviço e da Nota de Empenho, para fins de verificação da conformidade do produto a ser fornecido deverá ser de até 7 (sete) dias úteis, contados do recebimento da Nota de Empenho;

5.1.4. Prazo de entrega da integralidade dos quantitativos dos itens constantes na Ordem de Serviço e da Nota de Empenho deverá ser de até 20 (vinte) dias corridos, contados da

aprovação da amostra prévia.

5.1.5. Após a assinatura do Contrato e as nomeações do Gestor e Fiscais do Contrato, será realizada a reunião inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus Anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

5.2. Inspeções e Diligências

5.2.1. A execução do Contrato será acompanhada e fiscalizada pelo Fiscal Técnico do Contrato, especialmente designado. Sem prejuízo da plena responsabilidade da Contratada perante o TJCE e/ou a terceiros, os serviços estarão sujeitos a mais ampla e irrestrita fiscalização, a qualquer hora e em todos os locais. A presença do Fiscal Técnico do Contrato não diminui a responsabilidade da empresa por quaisquer irregularidades resultantes de imperfeições técnicas e não implicam corresponsabilidade do TJCE ou do Fiscal.

5.2.2. O Fiscal Técnico monitora os riscos inerentes à execução dos serviços. Para tanto, registra todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário à regularização das falhas.

5.2.3. Caso existam falhas que requeiram a aplicação de sanções, o Fiscal comunica ao Gestor do Contrato para que tome as devidas providências. Todas as decisões e ações que ultrapassem a competência do Fiscal Técnico devem ser solicitadas ao Gestor do Contrato em tempo hábil para adoção de medidas cabíveis.

5.2.4. Ao Fiscal Técnico fica assegurado o direito de exigir o cumprimento de todos os itens constantes do Termo de Referência, do Edital, da proposta e das cláusulas do Contrato.

5.2.5. Eventuais irregularidades deverão ser comunicadas pela Contratada, por escrito, ao Fiscal Técnico com os esclarecimentos julgados necessários e as informações sobre possíveis paralisações de serviços. Devem ser apresentados relatórios técnicos ou justificativas a serem apreciadas e decididas pelo Gestor do Contrato.

6. ELEMENTOS PARA GESTÃO DO CONTRATO

6.1. Papeis e Responsabilidade

Id	Papel	Entidade	Responsabilidade
01	Gestor do Contrato	Secretário(a) de Tecnologia da Informação do TJCE	Orientar e coordenar a fiscalização e o acompanhamento da execução do objeto contratual, prazos e condições estabelecidas neste documento e seus Anexos; Exigir da Contratada a correta execução do objeto e o exato cumprimento das obrigações assumidas, nos termos e condições

			previstas neste documento e seus Anexos, inclusive quanto às prestações acessórias; Encaminhar à Administração do Contratante relato circunstanciado de todos os fatos e ocorrências que caracterizem atraso e descumprimento de obrigações assumidas e que sujeitam a Contratada às sanções previstas neste documento, discriminando em memória de cálculo, se for o caso, os valores das multas aplicáveis; Na hipótese de descumprimento total ou parcial do contrato ou de disposição deste documento e seus Anexos, adotar imediatamente as medidas operacionais e administrativas necessárias à notificação da Contratada para o cumprimento imediato das obrigações inadimplidas; Analisar e manifestar-se sobre justificativas e documentos apresentados pela Contratada por atraso ou descumprimento de obrigação assumida, submetendo sua análise e manifestação à consideração da autoridade administrativa competente.
02	Fiscal Técnico	**SETIN** – Será indicado posteriormente e nomeado por portaria no Diário da Justiça do Estado do Ceará.	Avaliação da qualidade dos serviços realizados e justificativas, de acordo com os Critérios de Aceitação definidos em contrato; Identificação de não conformidade com os termos contratuais; Comunicar por escrito ao gestor do contrato qualquer falta cometida pela empresa contratada, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar a aplicação de sanção, advertência ou à rescisão contratual; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato;

			Realizar pessoalmente a medição dos serviços contratados; Recusar serviço ou fornecimento irregular ou em desacordo com condições previstas no termo de referência, na proposta da contratada e no contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados; Averiguar se é o contratado quem executa o contrato e certificar-se de que não existe cessão ou subcontratação, salvo se previamente autorizado pelo TJCE; Atestar a efetiva realização do objeto contratado para fins de pagamento das faturas correspondentes; Acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle da qualidade dos materiais, serviços e equipamentos a serem aplicados nos serviços.
03	Fiscal Requisitante do Contrato	**SETIN** – Será indicado posteriormente e nomeado por portaria no Diário da Justiça do Estado do Ceará.	Avaliação da qualidade dos serviços realizados e justificativas, de acordo com os Critérios de Aceitação definidos em contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Identificação de não conformidade com os termos contratuais, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Verificação da manutenção da necessidade, economicidade e oportunidade da contratação; Acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle da qualidade dos materiais, serviços e equipamentos a serem aplicados nos serviços, em conjunto com o Fiscal Técnico; Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de

			segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato, quando solicitado pelo Gestor do Contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Comunicar por escrito ao gestor do contrato qualquer falta cometida pela empresa contratada, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar a aplicação de sanção ou à rescisão contratual, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato.
04	Fiscal Administrativo	**SETIN** – Será indicado posteriormente e nomeado por portaria no Diário da Justiça do Estado do Ceará.	Providenciar a instrução administrativa do processo, fornecendo à contratada todas as orientações necessárias para a correta emissão de notas fiscais, de acordo com os serviços atestados pelos fiscais técnicos. Validar, por meio de recálculos, mas sem avaliação de aspectos técnicos, a apuração, realizada pelos fiscais técnicos e materializada no Termo de Recebimento Definitivo (TRD), da origem e do objeto do que se deve pagar, da importância exata a ser paga e a quem se deve pagar para extinguir a obrigação, com base no contrato, na nota de empenho e nos comprovantes de entrega do material ou da efetiva prestação do serviço, em conformidade com o disposto nos arts. 62 e 63 da Lei nº 4.320, de 18 de março de 1964; Efetuar o controle da vigência, realizando comunicado ao fiscal técnico em tempo hábil, uma vez que este deverá controlar os

			prazos de execução, necessidades de prorrogações ou nova contratação, ficando o fiscal administrativo responsável pelo controle da época de reajustamento dos preços contratados, tomando as providências cabíveis em tempo hábil junto à Coordenadoria de Central de Contratos e Convênios do TJCE, quando necessário; Verificar se a empresa contratada cumpriu com a garantia prevista no contrato.

6.2. Deveres e Responsabilidades da Contratante

6.2.1. Designar responsáveis para o acompanhamento e fiscalização da execução do objeto contratual;

6.2.2. Receber o objeto entregue pela Contratada, que esteja em conformidade com as especificações e com a proposta arrematante;

6.2.3. Estabelecer normas e procedimentos de acesso às suas instalações para a execução do objeto;

6.2.4. Informar à Contratada de atos que possam interferir direta ou indiretamente nos serviços prestados;

6.2.5. Comunicar formalmente qualquer anormalidade ocorrida na execução do objeto adquirido;

6.2.6. Aplicar à Contratada as sanções administrativas contratuais cabíveis;

6.2.7. Rejeitar o serviço em desconformidade ou incompatível com as especificações apresentadas;

6.2.8. Responsabilizar-se pelos pagamentos dos itens recebidos;

6.2.9. Permitir o acesso às dependências do TJCE, aos técnicos da Contratada, responsáveis pela execução dos serviços;

6.2.10. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da Contratada;

6.2.11. Efetuar o pagamento dos serviços de acordo com as condições contratuais, no prazo e condições estabelecidas neste Termo de Referência, e no caso de cobrança indevida, glosar os valores considerados em desacordo com o contrato.

6.3. Deveres e Responsabilidades da Contratada

6.3.1. Proceder, no prazo fixado em edital, a entrega do objeto, conforme especificações técnicas, quantidades, prazos e demais condições estabelecidas no Edital, na Proposta e no Termo de Referência, acompanhado da respectiva nota fiscal;

6.3.2. Quando no ambiente do TJCE, manter os seus funcionários sujeitos às normas disciplinares, porém sem qualquer vínculo empregatício com o Órgão;

6.3.3. Respeitar as normas e procedimentos de controle e acesso às dependências do TJCE;

6.3.4. Executar o objeto do certame em estrita observância dos ditames estabelecido pela Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)). Para a habilitação, o CONTRATADA deverá apresentar declaração indicando o encarregado da credenciada responsável pela proteção de dados, nos termos do art. 41 da Lei Federal 13.709/18;

6.3.5. Utilizar, exclusivamente, pessoal habilitado à prestação dos serviços, objeto deste documento;

6.3.6. Manter os seus funcionários e prepostos identificados por crachá, quando em trabalho, devendo substituir imediatamente qualquer um deles que seja considerado inconveniente à boa ordem e às normas disciplinares do TJCE;

6.3.7. Responder pelos danos causados diretamente à administração do TJCE ou a terceiros, decorrentes de sua culpa ou dolo, durante o fornecimento e a execução do objeto;

6.3.8. Arcar com despesa decorrente de qualquer infração seja qual for, desde que praticada por seus funcionários no recinto do TJCE;

6.3.9. Comunicar ao TJCE qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários;

6.3.10. Manter em compatibilidade com as obrigações a serem assumidas, durante toda a execução do contrato, todas as condições de habilitação e de qualificação na licitação;

6.3.11. Assumir as despesas decorrentes da execução do contrato e da garantia, bem como os encargos fiscais, taxas comerciais, tributos e contribuições que incidam direta ou indiretamente;

6.3.12. Indicar um preposto para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;

6.3.13. Na hipótese de afastamento do preposto definitivamente ou temporariamente, a CONTRATADA deverá comunicar ao Gestor do Contrato por escrito o nome e a forma de comunicação de seu substituto;

6.3.14. Sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do art. 65 da Lei n° 8.666/93, quais sejam, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor atualizado do contrato;

6.3.15. Cumprir fielmente o que estabelece este Termo de Referência, em especial no que se refere à implantação, operação e níveis de serviço;

6.3.16. Prestar todos os esclarecimentos técnicos solicitados pelo TJCE acerca das características e funcionamento do objeto.

6.4. Forma de Acompanhamento do Contrato

6.4.1. O Recebimento Provisório do objeto será dado pelo Fiscal do Contrato, em até 10 (dez) dias após a entrega dos equipamentos, compreendendo dentre outras, as seguintes verificações:

6.4.1.1. Os materiais deverão estar em suas respectivas embalagens originais, se cabível, com a indicação da marca/modelo na embalagem e/ou no próprio material, bem como das demais características que possibilitem a correta identificação do material;

6.4.1.2. Condições da embalagem e/ou do material;

6.4.1.3. Quantidade entregue;

6.4.1.4. Apresentação do documento fiscal, com identificação do fornecedor e do comprador (Tribunal), descrição do material entregue, quantidade, preços unitário e total;

6.4.2. O Recebimento Definitivo do objeto será dado pelo Fiscal de Contrato, após a emissão da Nota Fiscal, em até 30 (trinta) dias após a entrega dos equipamentos, satisfeitas as condições abaixo:

6.4.2.1. Correspondência de marca/modelo do material com os indicados na nota de empenho ou proposta da fornecedora;

6.4.2.2. Compatibilidade do material entregue com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa fornecedora;

6.4.2.3. Realização de testes, quando previstos no Termo de Referência ou caso a unidade recebedora entenda necessário;

6.4.2.4. Conformidade do documento fiscal quanto à identificação do comprador (Tribunal), descrição do material entregue, quantidade, preços unitário e total;

6.4.3. Para o aceite, os equipamentos e seus componentes serão submetidos, a critério da CONTRATANTE, a testes de desempenho e/ou demonstrações de funcionamento, que verificarão funções e parâmetros especificados neste Termo de Referência.

6.4.4. Para os serviços de instalação de software, configuração e transferência de conhecimento:

6.4.4.1. O Recebimento Provisório do objeto será dado pelo Fiscal do Contrato, em até 10 (dez) dias após a execução dos serviços, compreendendo dentre outras, a apresentação do relatório técnico com a descrição dos serviços executados;

6.4.5. O Recebimento Definitivo do objeto será dado pelo Fiscal de Contrato, após a emissão da Nota Fiscal, em até 30 (trinta) dias após a execução dos serviços, satisfeitas as condições abaixo:

6.4.5.1. Compatibilidade dos serviços executados com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa fornecedora;

6.4.5.2. Em caso de serviços de instalação e configuração, a entrega da solução em pleno funcionamento, conforme avaliado pela equipe técnica do Tribunal;

6.4.5.3. Em caso de treinamento, apresentar os certificados de conclusão do curso emitidos para os participantes;

6.4.5.4. Conformidade do documento fiscal quanto à identificação do comprador (Tribunal), descrição do serviço entregue, quantidade, preços unitário e total.

6.4.6. As ações pertinentes a execução do objeto da solução seguem dispostas no item **3 REQUISITO PRÉVIO PARA ADJUDICAÇÃO DO OBJETO; item 4 REQUISITOS DO PROJETO DE IMPLANTAÇÃO e item 5 REQUISITOS DE GARANTIA E MANUTENÇÃO presentes no AQSETIN2022015 – ANEXO I – Especificações**.

6.5. Metodologia de Avaliação da Qualidade

6.5.1. A execução e garantia do objeto serão acompanhados, fiscalizados e atestados por servidores designados pelos ordenadores de despesa da Administração, que também verificarão o exato cumprimento de todas as cláusulas e condições, inclusive a qualidade do objeto recebido, conforme prevê o art. 67 da Lei nº 8.666/93, além de atestar as faturas apresentadas pela CONTRATADA, devendo, ainda, fazer anotações e registros de todas as ocorrências, determinando o que for necessário à regularização das falhas ou defeitos observados;

6.5.2. O Fiscal anotará em registro próprio todas as ocorrências relacionadas com o fornecimento do objeto, bem como os serviços de entrega, instalação e garantia, determinando o que for necessário à regularização das faltas ou defeitos observados.

6.6. Níveis de Serviço

6.6.1. Os níveis mínimos de serviço descrevem a disponibilidade mínima que a CONTRATADA deve garantir em relação ao tempo de atividade ou continuidade dos serviços contratados. A aferição dos níveis de serviço será realizada por meio do indicador descrito no item **2.4 – Suporte Técnico Especializado, disposto no ANEXO I.**

6.7. Estimativa do Volume de Bens/Serviço

ID	Bem/Serviço	Estimativa
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	150
2	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	114
3	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	400
4	Suporte Técnico Especializado	24
5	Treinamento Técnico da Solução de Gerenciamento de Vulnerabilidades	8

6.8. Prazos e Condições

6.8.1. Dos acréscimos

6.8.1.1. A CONTRATADA deverá aceitar, nas mesmas condições propostas, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial do contrato.

6.8.1.2. Alteração contratual unilateral, pela Administração Pública, quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos conforme o artigo 65, inciso I, alínea a, da Lei nº 8.666, de 21 de junho de 1993, a Lei de Licitações e Contratos Administrativos.

6.8.2. Rescisão

6.8.2.1. Ficará o Contrato rescindido, mediante formalização, assegurado o contraditório e a defesa, nos seguintes casos:

6.8.2.1.1. Atraso injustificado na execução dos serviços contratados;

6.8.2.1.2. Paralisação dos serviços sem justa causa ou prévia autorização da Administração;

6.8.2.1.3. Subcontratação total ou parcial do Objeto deste Termo de Referência, associação da Contratada com outrem, cessão ou transferência total ou parcial, bem como da fusão, cisão ou incorporação que afetem a boa execução do Contrato;

6.8.2.1.4. Desatendimento das determinações da autoridade designada para acompanhar e fiscalizar a execução do Contrato, assim como a de seus superiores;

6.8.2.1.5. Cometimento reiterado de falhas na execução do Contrato;

6.8.2.1.6. Decretação de falência ou insolvência civil;

6.8.2.1.7. Dissolução da empresa;

6.8.2.1.8. Alteração ou modificação da finalidade ou da estrutura da Empresa que prejudiquem a execução do Contrato;

6.8.2.1.9. Ocorrência de caso fortuito ou força maior regularmente comprovados, impeditivos da execução do Contrato;

6.8.3. RESCISÃO, nos casos previstos no art.78 da Lei nº 8.666/93

6.8.3.1. Poderá, ainda, ser rescindido pelo CONTRATANTE, a qualquer tempo, mediante simples aviso à outra parte, com antecedência mínima de 30 (trinta) dias.

6.9. Condições para Pagamento

6.9.1. O aceite dos serviços prestados por força desta contratação será feito mediante ateste das Notas Fiscais, esta contendo nº da nota de empenho e/ou do contrato, para fins de ateste, liquidação e pagamento;

6.9.2. O pagamento será creditado em nome da CONTRATADA, em parcela única pelo CONTRATANTE e não havendo documentos a regularizar no prazo de até 10 dias consecutivos, contados da emissão do Termo de Recebimento Definitivo e Nota Fiscal/Fatura;

6.9.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

6.9.4. O adimplemento da obrigação será em moeda nacional.

6.9.5. Poderá haver a glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA não produziu os resultados acordados; deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida; deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

6.9.6. O item **6.6** baliza os percentuais de glosa em caso de irregularidades cometidas pela CONTRATADA;

6.9.7. Ocorrendo erros na apresentação da nota fiscal, esta será devolvida à CONTRATADA para correção, ficando estabelecido que o atraso decorrente deste fato implicará postergação da data do pagamento, por igual número de dias, sem que isto gere encargos

financeiros para o CONTRATANTE.

6.9.8. Nenhum pagamento será efetuado a contratada na pendência da atestação de conformidade da entrega do objeto, sem que isso gere direito a alteração de preços ou compensação financeira;

6.9.9. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pelo CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM: I x N x VP

EM= Encargos moratórios

N= Número de dias entre a data prevista para o pagamento e a do efetivo pagamento

VP= Valor da parcela a ser paga

I = Índice de atualização financeira = 0,0001644, assim apurado:

I= (T/100)/365 I= 0,0001644

TX= Percentual da taxa anual= %

6.10. Garantia

6.10.1. As especificações acerca da garantia da solução encontram-se dispostas no item 5. REQUISITOS DE GARANTIA E MANUTENÇÃO presente no ANEXO I – ESPECIFICAÇÕES TÉCNICAS deste documento.

6.11. Propriedade, Sigilo, Restrições

6.11.1. A CONTRATADA cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do art. 111, da Lei Federal N.º 8.666/93, combinado com o art. 4.º, da Lei Federal N.º 9.609/98, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência dos serviços contratados, entendendo-se por resultados quaisquer documentos, artefatos, arquivos, fluxos de trabalho, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida pelo TJCE utilizando a solução contratada, sendo vedado à CONTRATADA sua cessão, locação ou venda a terceiros;

6.11.2. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços da CONTRATADA ensejará a responsabilidade criminal, na forma da lei, sem prejuízo de

outras providências nas demais esferas;

6.11.3. A CONTRATADA deverá assinar termo de compromisso (ANEXO VI), constante com declaração de manutenção de sigilo e respeito às normas de segurança vigentes no órgão ou entidade em razão do trabalho vinculado ao contrato assinado;

6.11.3.1. Pela mesma razão a CONTRATADA deverá providenciar o Termo de Ciência (ANEXO V) da Declaração de Manutenção de Sigilo e respeito às normas vigentes no órgão ou entidade, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, quando assim se fizer necessário.

6.12. Mecanismos Formais de Comunicação

ID	Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
1	Emissão da Ordem de serviço/fornecimento de bens	Contratante	Contratada	Ordem de serviço/fornecimento de bens	Quando demandado pela SETIN.
2	Emissão da Nota de Empenho	Contratante	Contratada	Nota de empenho	Quando demandado pela SETIN.
3	Abertura de chamados da garantia. Dirimir dúvidas e prestar esclarecimentos acerca de itens presentes no contrato firmado;	Contratante	Contratada	E-mail, telefone e site na internet	Sempre que necessário.
4	Registro das reuniões realizadas entre a contratante e a contratada.	Contratante	Contratada	Ata de reunião	Sempre que houver reunião entre as partes.
5	Relato de alguma ocorrência contratual através de Ofício por correspondência.	Contratante	Contratada	Ofício	Sempre que houver falha no atendimento a algum item do contrato ou quando necessário.
6	Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, e-mail, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet, PDF (*Portable Document Format*): documento em formato	Quando necessário

				portável.	

7. ESTIMATIVA DE PREÇO

Id	Bem/Serviço	QTD	Unidade de Medida	Valor Unitário	Valor Total
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	150	Licenças	**R$ 1.150,00**	**R$ 172.500,00**
2	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	114	Licenças	**R$ 1.204,00**	**R$ 137.256,00**
3	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	400	Licenças	**R$ 1.453,00**	**R$ 581.200,00**
4	Suporte Técnico Especializado	24	Meses	**R$ 10.000,00**	**R$ 240.000,00**
5	Treinamento Técnico da Solução de Gerenciamento de Vulnerabilidades	8	Voucher por usuário	**R$ 8.600,00**	**R$ 68.800,00**
Total					**R$ 1.199.756,00**

8. ADEQUAÇÃO ORÇAMENTÁRIA

Fonte	FUNDO ESPECIAL DE REAPARELHAMENTO E MODERNIZAÇÃO DO JUDICIÁRIO – FERMOJU
Programa	512 - EXCELÊNCIA NO DESEMPENHO DA PRESTAÇÃO JURISDICIONAL
Período	2023~2024

It	Valor	Tipo	Natureza	Valor
1	Solução de Gerenciamento de vulnerabilidades para FQDNs Externos, dos ativos de Tecnologia da Informação, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	Serviço	INVESTIMENTO	**R$ 172.500,00**
2	Solução de Gerenciamento de vulnerabilidades para Imagens de aplicações em Container, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	Serviço	INVESTIMENTO	**R$ 137.256,00**
3	Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses.	Serviço	INVESTIMENTO	**R$ 581.200,00**
4	Suporte Técnico Especializado	Serviço	**CUSTEIO**	**R$ 240.000,00**
5	Treinamento Técnico da Solução de Gerenciamento de Vulnerabilidades	Serviço	**CUSTEIO**	**R$ 68.800,00**
Total				**R$ 1.199.756,00**

9. Sanções Aplicáveis

9.1.1. O descumprimento das disposições contratuais poderão sujeitar a Contratada as seguintes sanções:

9.1.1.1. Advertência;

9.1.1.2. Impedimento de licitar e contratar com a União, e, ainda, descredenciamento no

sistema de cadastramento de fornecedores do Tribunal e do SICAF, pelo prazo de até 5 (cinco) anos, nas hipóteses contempladas no Edital do Pregão;

9.1.1.3. Declaração de inidoneidade para licitar ou contratar com a Administração Pública Estadual;

9.1.1.4. Multa:

9.1.1.4.1. Multa de até 0,5% (zero vírgula cinco por cento), por dia corrido de atraso, até o limite de 15 (quinze) dias de atraso, sobre o valor total do contrato em caso de atraso injustificado na entrega do objeto;

9.1.1.4.2. No caso de atraso injustificado na entrega dos serviços por prazo superior a 20 (vinte) dias corridos, com a aceitação pela Administração, será aplicada a multa de 10% sobre o valor da Ordem de Fornecimento.

9.1.1.4.3. Decorrido o prazo de 30 (trinta) dias de atraso injustificado na entrega e/ ou na solução de chamado de atendimento, será caracterizada a inexecução parcial do contrato. Com a aceitação pela Administração, será aplicada a multa de 10% sobre o valor do contrato.

9.1.1.4.4. Decorrido o prazo de 45 (quarenta e cinco) dias de atraso injustificado na entrega e/ou na solução de chamado de atendimento, será caracterizada a inexecução total do contrato.

9.1.1.4.5. Multa de até 10% sobre o valor total do Contrato, em caso de inexecução parcial do contrato;

9.1.1.4.6. A inexecução parcial do contrato se caracterizará na situação de decorrido o prazo de 15 (quinze) dias de atraso injustificado nos prazos de entrega do objeto, sem prejuízo dos demais motivos previstos em lei.

9.1.1.4.7. A inexecução total do contrato se caracterizará na situação de decorrido o prazo de 30 (trinta) dias de atraso injustificado nos prazos de entrega do objeto, sem prejuízo dos demais motivos previstos em lei.

9.1.1.4.8. Nos casos em que a CONTRATADA não atender aos indicadores de níveis de serviço indicados no item **2.4 Suporte Técnico Especializado presente no ANEXO I – ESPECIFICAÇÕES TÉCNICAS** deste documento, a mesma incorrerá às glosas definidas na tabela presente no respectivo item;

9.1.2. A CONTRATADA estará ainda sujeita a:

9.1.2.1. RESCISÃO, nos casos previstos no art.78 da Lei nº 8.666/93.

9.1.2.2. Ao TJCE será assegurado, após regular processo administrativo, utilizar a garantia para permitir a compensação da multa aplicada.

9.1.3. As multas e sanções legais poderão ser aplicadas conjuntamente, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 5 (cinco) dias úteis, a serem aplicadas pela autoridade competente;

9.1.4. Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA;

9.1.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993 e, subsidiariamente, a Lei nº 9.784, de 1999.

9.1.6. As multas devidas e/ou prejuízos causados ao CONTRATANTE serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

9.1.7. Caso o CONTRATANTE determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente;

9.1.8. As notificações de multas e sanções são de responsabilidades da Divisão Central de Contratos e Convênios do TJCE que receberá dos setores responsáveis os relatórios com as ocorrências insatisfatórias que comprometam a execução do contrato.

9.1.9. A autoridade competente para apreciar o recurso poderá, motivadamente e presentes razões de interesse público, dar eficácia suspensiva ao recurso interposto pela CONTRATADA.

9.1.10. A aplicação de quaisquer penalidades previstas no edital e seus anexos serão obrigatoriamente registradas no SICAF e precedida de regular processo administrativo, onde será assegurado o contraditório e a ampla defesa, sem prejuízo das responsabilidades civil e criminal, ressalvados os casos devidamente justificados e acatados pelo Tribunal.

10. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Proposta de Preço

10.1.1. A proposta deverá conter obrigatoriamente os seguintes elementos:

10.1.1.1. Preço unitário por item, em moeda corrente nacional, cotados com apenas duas casas decimais, expressos em algarismos e por extenso, sendo que, em caso de divergência entre os preços expressos em algarismos e por extenso, serão levados em consideração os últimos;

10.1.1.2. Não deve conter cotações alternativas, emendas, rasuras ou entrelinhas;

10.1.1.3. Deve fazer menção ao número do pregão e do processo licitatório;

10.1.1.4. Deve ser datada e assinada na última folha e rubricadas nas demais, pelo representante legal da empresa;

10.1.1.5. Deve conter na última folha o número do CNPJ da empresa;

10.1.1.6. Deve informar o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, contados da data de entrega da mesma;

10.1.1.7. Deverá conter a descrição detalhada do objeto, tais como: somente uma única marca, modelo, características do objeto, procedência e demais dados que a CONTRATADA julgar necessário;

10.1.1.8. Indicação do nome do banco, número da agência, número da conta-corrente, para fins de recebimento dos pagamentos.

10.1.1.9. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais o direito de acesso aos dados constantes dos sistemas;

10.1.1.10. A licitante vencedora deve preencher os preços do(s) modelo(s) de proposta de preços, disposto no ANEXO IV, do(s) item(s) em que for vencedora, conforme lances.

10.2. Critérios de Seleção

10.2.1. Tipo de Licitação

10.2.1.1. O critério de julgamento adotado será o MENOR PREÇO, observadas as exigências contidas neste documento e seus anexos quanto às especificações do objeto;

10.2.1.2. Por tratar-se de execução complexa, compreendendo o fornecimento de materiais e a execução dos serviços de implantação da solução, sob inteira responsabilidade da CONTRATADA, caracteriza-se o fornecimento do objeto por meio de empreitada integral, em conformidade com a alínea "e" do inciso II do art. 10 da LEI Nº 8.666 DE 21 DE JUNHO DE 1993..

10.3. Justificativa de Adoção da Modalidade da Licitação

10.3.1. Modalidade de Licitação

10.3.1.1. A modalidade de licitação escolhida deve ser o Pregão na forma eletrônica, sob o modo de disputa aberto, considerando se tratar de bens e serviços comuns, nos termos da lei Federal n° 10.520/2002, vez que seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo Termo de Referência e Edital, por meio de especificações usuais no mercado.

10.4. Qualificação Econômico-Financeira

10.4.1. Certidão negativa de falência expedida pelo distribuidor da sede do licitante;

10.4.2. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da

proposta;

10.4.3. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

10.4.4. É admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

10.4.5. Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

LG =	Ativo Circulante + Realizável a Longo Prazo
	Passivo Circulante + Passivo Não Circulante
SG =	Ativo Total
	Passivo Circulante + Passivo Não Circulante
LC =	Ativo Circulante
	Passivo Circulante

10.4.6. As empresas, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor total estimado do grupo pertinente.

10.5. Qualificação Técnica

10.5.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a serviços executados com as seguintes características mínimas:

10.5.1.1. Para a habilitação, a licitante detentora da melhor proposta deverá apresentar, no mínimo, 1 (um) atestado de capacidade técnica, emitido por pessoa jurídica de direito publico ou privado nacional, que comprove que a licitante possui capacidade técnico-operacional e aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente;

10.5.1.2. O TJCE se resguarda no direito de diligenciar junto à pessoa jurídica emitente do atestado/declaração de capacidade técnica, visando a obter informações sobre os produtos fornecidos e/ou serviços prestados, cópias dos respectivos contratos/aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

11. GARANTIA CONTRATUAL

11.1. No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do CONTRATANTE, contados da assinatura do contrato, a contratada deverá apresentar comprovante de prestação de garantia, para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, no percentual de 3% (três por cento) do valor total do contrato,

podendo a mesma optar por qualquer das modalidades previstas no art. 56 da Lei 8.666/93, a saber:

11.1.1. Caução em dinheiro ou títulos da dívida pública, cuja exigibilidade não seja contestada pelo TJCE;

11.1.2. Quando se tratar de caução em dinheiro, deverá ser recolhido na Secretaria de Finanças do TJCE;

11.1.3. Seguro garantia;

11.1.3.1. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria;

11.1.4. Fiança bancária;

11.1.4.1. Em se tratando de fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil.

11.1.5. Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a Contratada deverá reintegralizar o seu valor, no prazo não superior a 15 (quinze) dias úteis, contados da data em que for notificada;

11.1.6. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

11.1.7. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

11.1.8. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger o período de vigência contratual.

11.1.9. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

11.1.9.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

11.1.9.2. Prejuízos diretos causados à Administração, decorrentes de culpa ou dolo durante a execução do contrato;

11.1.9.3. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

11.1.9.4. Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

11.1.9.5. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

11.1.10. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

12. VIGÊNCIA CONTRATUAL

12.1. A vigência do contrato inicia na data de assinatura do contrato e vigorará:

12.2. Para o fornecimento da solução a ser adquirida por até 70 (setenta) dias corridos, conforme previsto na tabela de Requisitos temporais, item **4.3** neste **TRF**. A contar da data de assinatura do contrato.

12.3. Para o serviço de suporte técnico especializado, por até 24 (vinte e quatro) meses, a contar da data emissão do Termo de Recebimento Definitivo, podendo ser prorrogado até 60 (sessenta) meses, com base no inciso IV do artigo 57, da Lei 8.666, de 1993, dado que se trata de serviço continuado.

12.4. Para a garantia da solução, por até 60 (sessenta) meses, contados da data de emissão do Termo de Recebimento Definitivo.

13. APROVAÇÕES

Aprovo. Encaminha-se à Comissão Permanente de Contratação para iniciação de procedimento licitatório, segundo o art. 38 da Lei nº 8.666 de 21 de junho de 1993.

Fortaleza, 21 de novembro de 2022.

Equipe de Planejamento da Contratação

Fábio de Carvalho Leite Matrícula: 9594 Integrante Administrativo	Adarildo de Brito Figueiredo Matrícula: 8025 Integrante Requisitante	Heldir Sampaio Silva Matrícula: 9630 Integrante Técnico

Cristiano Henrique Lima de Carvalho – Matrícula nº 5198
Autoridade Competente da Área Administrativa, em substituição.