**ESTADO DO CEARÁ**
**PODER JUDICIÁRIO**
**SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO**

# ESTUDOS TÉCNICOS PRELIMINARES – ETP

*O presente Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.*

**AQSETIN2022015 – Solução de gestão e análise de vulnerabilidades de ativos**

## 1. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO (Art. 14, I)

A estudo tem por objetivo analisar a viabilidade técnica e econômica da contratação de empresa especializada no fornecimento de uma **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 prestação dos serviços de Consultoria Especializada, suporte, com garantia (manutenção e suporte técnico), incluindo a garantia de atualização das versões**. A contratação deverá compreender o período de 12 (doze meses), podendo ser prorrogada de acordo com o estabelecido legalmente. As especificações, funcionalidades e quantidades serão definidas e justificadas em momento oportuno, neste documento de estudo técnico.

## 2. REQUISITOS DE NEGÓCIO DA ÁREA REQUISITANTE (Art. 14, I)

### 2.1. Necessidades de Negócio

**2.1.1.**O ambiente tecnológico do TJCE é composto por vários ativos tecnológicos, sistemas legados e um grande número de usuários desses recursos, tais como:

| 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 Midias |
| 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 administrtivos: |
| Sites de admrh (portal) |
| Themis |
| Portal Adm (Ead) |
| Spes |
| ssas |
| Espaço do Servidor |
| webmail |
| Catinet (Versão externa) |
| CatiWeb (Versão externa) |
| Sasr |
| Proceso Administrativo – CPA |
| VDC |
| Sites de aplicativos / sistemas |
| Sites de informações gerais |

### 2.1.2.IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

**2.1.2.1.** 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;<br>Gerenciamento de Vulnerabilidades em ativos e Sistemas Operacionais;<br>Gerenciamento de Vulnerabilidades em Sistemas e páginas WEB;<br>Detecção e Correção de falhas de softwares que possam acarretar riscos na segurança, na funcionalidade e no desempenho dos sistemas;<br>Implantação de mecanismos para realizar o bloqueio de ataques constantes;<br>Foco na melhoria constante do sistema de segurança de dados corporativos;<br>Auxílio na implementação de políticas de segurança;<br>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;<br>Solução de análise de vulnerabilidades e Serviços técnicos especializados na área de Segurança da Informação;<br>Análise de Vulnerabilidades;<br>Gerenciamento de patches;<br>Gerenciamento da configuração de segurança;<br>Auditoria de software de alto risco;<br>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;<br>Otimização dos processos de infraestrutura da TIC conforme as melhores práticas;<br>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;<br>Testar as aplicações e páginas web, internas e externas, comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança por grandes fabricantes de software;<br>Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas.<br>Aumento da proteção dos ativos de informação do TJCE. |

**2.1.3.** Seguem definidas no **ANEXO I** demais especificações técnicas da solução.

**2.2. Demais Requisitos**

**2.2.1.**Seguem definidos no **ANEXO I** os requisitos atinentes à:

**2.2.1.1.** Capacitação;

**2.2.1.2.** 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;<br><br>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;<br><br>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);<br><br>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:<br><br>
<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 da Solução.</td><td>CONTRATADA</td><td>Até 30 (trinta) dias após o evento 1.</td></tr>
<tr><td>3</td><td>Conferência dos componentes da solução.</td><td>CONTRATANTE</td><td>Até 05 (cinco) dias após o evento 2.</td></tr>
<tr><td>4</td><td>Entrega do Plano de Implantação.</td><td>CONTRATADA</td><td>Até 10 (dez) dias após o evento 1.</td></tr>
<tr><td>5</td><td>Aceite do Plano de Implantação.</td><td>CONTRATANTE</td><td>Até 05 (cinco) dias após o evento 4.</td></tr>
<tr><td>6</td><td>Implantação da Solução –</td><td>CONTRATADA</td><td>Até 10 (dez) dias úteis após o evento 3.</td></tr>
</table></td></tr>
</table>

| | | | | |
|---|---|---|---|---|
| | | Homologação.* | | |
| | **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:**<br>• 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;<br>• 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.<br>**Quanto ao cerne das funcionalidades do objeto, são almejados como requisitos:**<br>• Gerenciamento de ameaças, como filtragem de mensagens e anti-malware;<br>• 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;<br>**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).<br>A CONTRATADA deve cumprir o disposto no inciso XXXIII do art. 7o da Constituição Federal de 1988, quanto ao emprego de menores.<br>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).<br>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. | | | |

## 3. LEVANTAMENTO DAS ALTERNATIVAS

**3.1.** Este estudo técnico identificou três soluções possíveis para o Gerenciamento de Vulnerabilidades:

### 3.1.1. 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.<br><br>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.<br><br>A rede estabelecida cria um complexo sistema de garantias econômicas, políticas e relações sociais que envolvem diversas esferas da sociedade.<br><br>O software, neste contexto, não é apenas um produto, mas também um artefato, por meio do qual, seus criadores proporcionam novos referenciais de produção.<br><br>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.<br>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. |

### 3.1.2. 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.<br><br>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.<br>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.<br><br>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.<br><br>Assim, como se vê a solução proposta não atende grande parte das necessidades tecnológicas e de negócio requeridas pelo TJCE. |

### 3.1.3. 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;**<br>**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).<br>Essa solução apresenta facilidade de gerenciamento, valor de aquisição adequado e atualização automática da plataforma.<br>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.<br>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. |

### 3.2. SOLUÇÕES PAGAS DISPONÍVEIS NO MERCADO

#### 3.2.1. F-Secure Elements Vulnerability Management.

**3.2.1.1.** 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.

#### 3.2.2. Qualys Vulnerability Management.

**3.2.2.1.** 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.

#### 3.2.3. Rapid7 InsightVM.

**3.2.3.1.** 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.

## 4. ANÁLISE DAS ALTERNATIVAS EXISTENTES (Art. 14, II, a – f)

| Requisito | ID da Solução | Sim | Não | N/A |
|---|---|---|---|---|
| A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal? | 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 no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário? | 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 definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)? | 1 | | | X |
| | 2 | | | X |
| | 3 | | | X |

## 5. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA (Art. 14, III e IV)

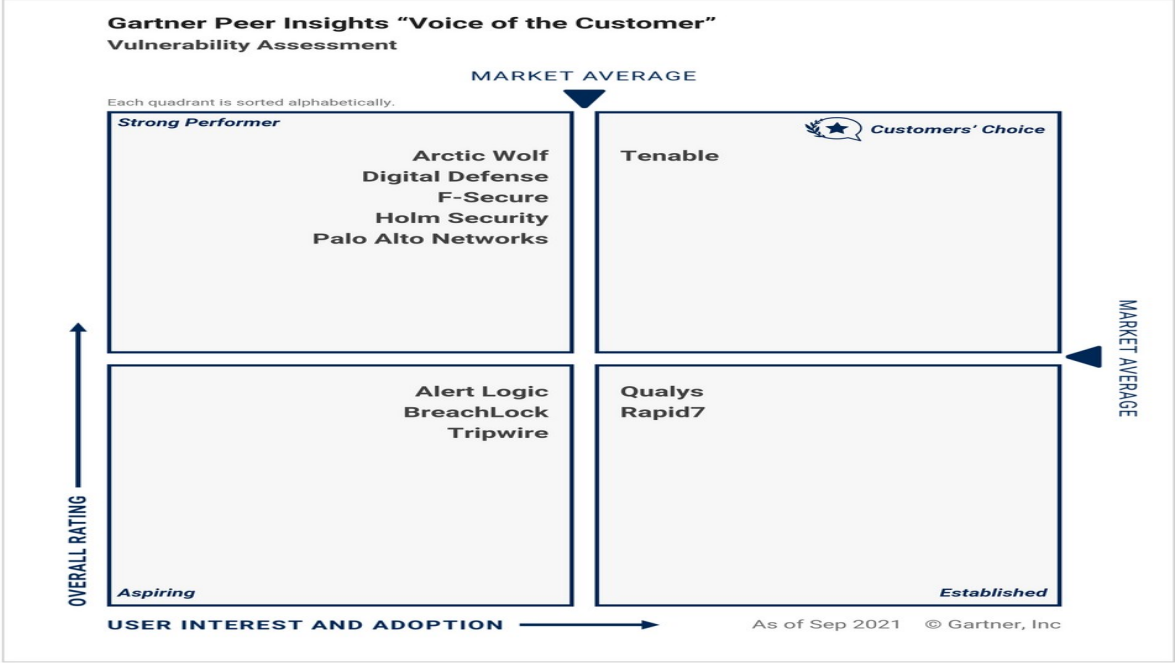
### 5.1. Identificação

**5.1.1.** Cenário 3 – 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 Estudo e seus anexos.

### 5.2. Justificativa

**5.2.1.** 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.




**5.2.2.** 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.

**5.2.3.** A análise das soluções levou em consideração:

**5.2.3.1.** As alternativas do mercado;

**5.2.3.2.** A existência de software público brasileiro;

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

**5.2.3.4.** As necessidades de adequação do ambiente do TJCE para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

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

**5.2.3.6.** Os diferentes modelos de prestação do serviço;

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

### 5.2.4. 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 | 114 | R$ 1.378,00 | R$ 157.092,00 |

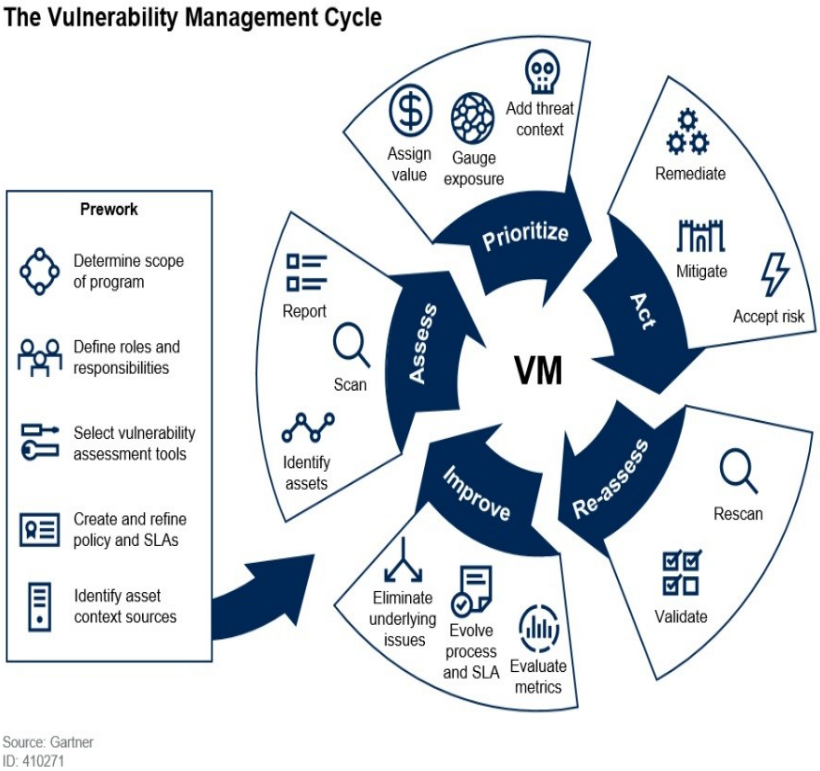
| | | | | |
|---|---|---|---|---|
| | também o de garantia dos equipamentos e/ou softwares pelo período de 60 meses. | | | |
| 3 | Solução de Gerenciamento de vulnerabilidades para Endpoints, baseada e com análise contínua e adaptável de riscos e confiança, com o serviço de implantação e também o de 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.**

**5.2.5.** 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 REQUISITOS DE NEGÓCIO DA ÁREA REQUISITANTE**; **3 LEVANTAMENTO DAS ALTERNATIVAS**.

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




**5.2.7.** Com base neste levantamento, os cenários descritos no item **3** apontam as soluções possíveis para atendimento da necessidade.

**5.2.8.** Conforme indicado no item **3**, os **cenários 1 e 2** se mostram insuficientes para o atendimento da demanda do TJCE de forma plena.

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

**5.2.9.1.** Não existe solução disponível no Portal do Software Público Brasileiro.

**5.2.10. CENÁRIO 2 – Utilização de softwares livres.**

**5.2.10.1.** A solução proposta atende apenas parte da necessidade, pois a utilização desse cenário implica 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.

**5.2.11.** 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 na tabela que seguem abaixo. Ao passo que, em observância ao princípio da economicidade, indica-se que a contratação da solução proposta deve ocorrer mediante adesão à referida ARP.

| ATA DE REGISTRO DE PREÇOS Nº 005/2022 - PE Nº 04/2022 – TRT 8ª REGIÃO | | | | |
|---|---|---|---|---|
| **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$ 1.150,00** | **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 | **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 | **R$ 1.453,00** | **R$ 581.200,00** |
| 4 | Suporte Técnico Especializado | 24 | **R$ 10.000,00** | **R$ 240.000,00** |
| 5 | Treinamento técnico da Solução de Gerenciamento de vulnerabilidades. | 8 | **R$ 8.600,00** | **R$ 68.800,00** |
| | | | **VALOR GLOBAL** | **R$ 1.199.756,00** |

**5.3. Descrição (Art. 14., IV, a)**

**5.3.1.** 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 Estudo e seus anexos.

**5.4. Estimativa de Custo Total da Contratação (Art. 14., IV, a)**

| 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$ 1.150,00** | **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 | **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 | **R$ 1.453,00** | **R$ 581.200,00** |
| 4 | Suporte Técnico Especializado | 24 | **R$ 10.000,00** | **R$ 240.000,00** |
| 5 | Treinamento técnico da Solução de Gerenciamento de vulnerabilidades. | 8 | **R$ 8.600,00** | **R$ 68.800,00** |
| | | | **VALOR GLOBAL** | **R$ 1.199.756,00** |

**5.5. Alinhamento em relação às necessidades de negócio e requisitos tecnológicos (Art. 14., IV, b)**

**5.5.1.** Corroborando com o referido alinhamento, é oportuno citar o item **5.4 RESULTADOS PRETENDIDOS**, extraído do DOD. Resultados estes que balizam as especificações da solução e equaliza-os com as demandas da Área de

Negócio.

**5.6. Benefícios Esperados (Art. 14., IV, c)**

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

**5.6.2. 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;

**5.6.3. 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;

**5.6.4. 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;

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

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

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

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

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

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

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

**5.6.8.** A equipe de planejamento da contratação, com base na avaliação de todos os elementos que compõem o presente estudo (necessidade de negócio e tecnológicas, requisitos da solução demandada pelo TJCE, comparação entre as soluções existentes, comparação entre as soluções viáveis em termos de custos, normativos pertinentes, contratações interdependentes, histórico das contratações do objeto e qualidade dos serviços a contratar) conclui pela viabilidade da contratação do objeto pelo TJCE.

**5.7. Relação entre a demanda e a quantidade**

**5.7.1.** Para estimar a quantidade de bens e serviços necessários que compõem a solução, faz-se necessário entender as funcionalidades das ferramentas de gestão de vulnerabilidades, bem como, modelo de licenciamento e a estratégia de segurança da informação da Secretaria de Tecnologia da Informação (SETIN).

**5.7.2.** Um dos principais componentes das soluções de gestão de vulnerabilidades é o *scan* de vulnerabilidade, que tem por objetivo identificar os riscos e vulnerabilidades externas e internas de uma rede. Tal ferramente realiza varredura em IP's externos ou ativos na rede interna, tipificando vulnerabilidades por riscos, identificando e classificando as possíveis falhas de segurança presentes na rede.

**5.7.3.** Trata-se de uma ferramenta eficaz, pois opera de maneira constante, detectando qualquer alteração que acontece dentro de um período especificado pelos gestores técnicos.

**5.7.4.** No caso das verificações de vulnerabilidades externas, são identificadas ameaças de maior gravosidade à rede, conferindo atualizações de softwares e *firmwares* necessárias para manutenção, portas e protocolos, ou seja, os pontos de falhas no *firewall* de rede.

**5.7.5.** Já a varredura da vulnerabilidade interna, como o nome indica, tem como objetivo a verificação de credenciais para efetuar login no dispositivo e executar verificações de conformidade e vulnerabilidades.

**5.7.6.** Além dessas estratégias, o *scan* utiliza a requisição ativa e passiva de informações. A aquisição ativa compreende em enviar um grande número de pacotes, possuindo pontos característicos, que, na maior parte do tempo, não seguem as recomendações, analisando as respostas para determinar a versão da aplicação utilizada. Com efeito, cada aplicação utiliza os protocolos de uma maneira ligeiramente diferente, que permite distingui-los.

**5.7.7.** A requisição passiva, menos intrusiva, apresenta menos riscos de ser detectada por um sistema de detecção de intrusos, o *IDS*, que funciona analisando os campos dos *datagramas* IP que circulam sobre uma rede, com a ajuda de um *sniffer*.

**5.7.8.** A caracterização, na versão passiva, analisa a evolução dos valores dos campos sobre séries de fragmentos, o que implica um tempo de análise muito mais longo, implicando uma análise mais difícil, ou mesmo impossível de detectar.

**5.7.9.** Como visto, a análise de vulnerabilidade objetiva detectar falhas em diversos componentes como: aplicações, softwares, equipamentos, sistemas operacionais, dentre outros.

**5.7.10.** Deve-se fazer continuamente o processo de verificação e análise da rede, para que a mesma fique sempre atualizada e livre de acessos não permiti dos e indesejáveis. Essa análise pode ser feita local e/ou remota.

**5.7.11.** Após tal análise são oferecidos relatórios com as respectivas soluções propostas. Nesses relatórios podem constar também itens dos quais objetiva-se melhorar a segurança do ambiente, não necessariamente relacionados às falhas encontradas. Divide-se em dois tipos:

**5.7.11.1.** Ativa – Encontra-se e corrige-se as falhas, emitindo relatórios apenas do que foi feito.

**5.7.11.2.** Passiva – Encontra-se as falhas e emite-se relatórios para que o cliente se encarregue de corrigir.

**5.7.12.** O relatório de análise de vulnerabilidades é constituído de informações essenciais que indicam a melhor estratégia para manter o ambiente do TJCE protegido de falhas, ataques e invasões, através de uma avaliação completa, auxiliando de uma forma mais fácil e assertiva a tomada de decisão em relação à segurança da informação.

**5.7.13.** Conforme relatório técnico (Chamado nº R1223747) da CATI – Grupo Resolvedor 3N, o TJCE possui os seguintes ativos a serem geridos, no tocante a vulnerabilidades:

| **RESUMO DA QUANTIDADE DE ATIVOS DO TJCE** | |
|---|---|
| **CATEGORIA** | **QUANTIDADE** |
| FQDNs | 458 |
| Appliance de Segurança | 236 |
| Ativos de Armazenamento | 8 |
| Ativos de Rede | 735 |
| Conteiners | 152 |
| Endpoints | 7289 |
| Hosts Físicos no Datacenter | 43 |
| Impressoras | 4 |
| Servidores de Aplicação | 453 |
| Sistema Operacional de Servidores | 1118 |

**5.7.14.** As informações foram extraídas através do relatório de ativos, que, em sua versão completa segue disposta de forma analítica no **AQSETIN2022015 – ANEXO II – Relatório de Ativos**.

**5.7.15.** Devido a grande quantidade de endereços IP's e de ativos de informação do TJCE, conforme mencionado neste, a estratégia de segurança da informação da SETIN, visa priorizar em primeiro momento a proteção dos ativos estratégicos do TJCE. Deve-se ter em mente que os ativos críticos do TJCE são os ativos que permitem a sua diferenciação face aos demais ativos e a sustentação do negócio a longo prazo.

**5.7.16.** Considerando que o modelo de licenciamento, baseia-se na quantidade de endereços IP's escaneados e considerando o exposto nas tabelas acima, acrescidos de uma previsão de crescimento de 10% (dez) por cento, estima-se que a quantidade de 174 licenças necessárias para IP's, número arredondado para fins de cálculo.

**5.7.17.** A previsão de crescimento é baseada na quantidade de aquisições de equipamentos previstas no PDTIC 2021-2022, na implantação de novos sistemas Web, aplicações e soluções que requerem a instalação de novas máquinas virtuais.

**5.7.18.** O quantitativo de licenças deverá ocorrer de forma a permitir o rodízio ao longo do ano, para os itens de configuração-IC's do TJCE, não sendo necessário, a ativação/licenciamento de todos os itens.

**5.7.19.** Quanto ao Suporte Técnico Especializado, esse deverá compreender o período de 60 (sessenta) meses.

**5.7.20.** Para a capacitação da equipe que deverá gerir a solução, deverá estar disponível até 08 (oito) unidades de treinamentos de forma atender 01 (hum) integrante da área de segurança da informação e 07 (sete) da área de Infraestrutura de TI.

## 6. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL (Art. 14, V)

**6.1.** Considerando o serviço que está sendo contratado, de forma intrínseca, o mesmo dispensa adequações do ambiente para recepcioná-lo.

## 7. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO (Art. 15, I)

### 7.1. Recursos Materiais

**7.1.1.** Levando em consideração a utilização da solução, em sua grande parte de forma remota, o acesso à Internet é recurso tecnológico essencial para viabilizar o seu uso e para que o suporte seja prestado nos termos especificados neste estudo preliminar.

**7.1.2.** Os demais recursos materiais necessários para uso e para a infraestrutura da solução já estão disponíveis e dimensionadas adequadamente no ambiente do TJCE.

**7.1.3.** A licitante deverá dimensionar os demais recursos necessários à prestação dos serviços, levando-se em consideração as condições constantes na solução.

## 8. ESTRATÉGIA DE CONTINUIDADE CONTRATUAIS (Art. 15, II)

### 8.1. No caso de interrupção do contrato:

**8.1.1.Cenário 1:** Implantar o uso emergencial e temporário de ferramenta livre e planejar novas licitações

para cobrir os diversos serviços não cobertos pela solução. Para algumas funcionalidades, seria necessário flexibilizar, em muito, os padrões de segurança da rede, de modo a ser possível utilizar serviços gratuitos (aqueles que sejam de uso livre, mesmo em ambiente empresarial), até que fosse possível contratar novos serviços que atendessem aos padrões mínimos de segurança e funcionalidades hoje já utilizados pelo TJCE.

**8.2. No caso de proximidade do final da vigência do contrato:**

**8.2.1.** Elaborar planejamento, com antecedência mínima de 9 (nove) meses, para verificar a necessidade/possibilidade de: contratação da renovação das licenças adquiridas.

**8.3.** Uma vez informado o cenário acima, devem ser ponderadas as seguintes informações acerca das responsabilidades da Empresa Fornecedora:

**8.3.1.** Tratando o presente objeto, uma vez contratado, deverá ser garantido exclusivamente pelo fabricante, não há expectativa razoável de descontinuidade do fornecimento do mesmo, a não ser a inexecução das condições contidas nos respectivos serviços, em cujo caso deverão ser iniciadas a ações legais cabíveis.

**8.3.2.** Efetuado o fornecimento, a responsabilidade pela continuidade dos serviços passará a ser do fabricante, na sua qualidade de emissor das licenças de serviços fornecidos pela licitante, sem prejuízo da responsabilidade da licitante, no caso que se constate qualquer irregularidade na aquisição e comercialização desses pacotes.

**8.4. Encerramento Abrupto do Contrato:**

**8.4.1.** Sendo o fornecimento dos serviços de forma única e imediata e sendo a execução dos mesmos de responsabilidade exclusiva do fabricante, não há possibilidade de encerramento abrupto por parte da licitante, a não ser a inexecução do fornecimento e/ou dos serviços a ele associados.

## 9. AÇÕES PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL (Art. 15, III)

**9.1.** As ações de redundância atendem as atividades pertinentes ao encerramento contratual e estão dispostas no item **8.**

## 10. ESTRATÉGIA DE INDEPENDÊNCIA (Art. 15, IV)

**10.1.** Em consonância com o Art. 15, IV da RESOLUÇÃO Nº 182 do Conselho Nacional de Justiça (CNJ) a licitante deverá observar os itens que seguem:

**10.1.1.** A forma de transferência de conhecimento tecnológico deverá ocorrer através de referências (hiperlinks dos sítios de internet) dos desenvolvedores das soluções contendo documentações básicas de utilização (manuais do usuário) dos itens entregues, e também as documentações de administração da solução pelo pessoal técnico de TI.

**10.1.2.** Como estratégia de independência, o objeto deverá ofertar suporte para a transposição de arquivos, e-mails, videoconferências para outras plataformas

**10.2. Transferência de Conhecimento (Art. 15, IV, a)**

**10.2.1.** O item **2.2.1.1**, traz em seu bojo as diretrizes de treinamento da equipe que gerirá a solução.

**10.3. Direitos de Propriedade Intelectual (Lei Nº 9.610, de 19 de fevereiro de 1998) (Art. 15, IV, b)**

**10.3.1.** A licitante 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 licitante, sendo vedado à licitante sua cessão, locação ou venda a terceiros.

**10.3.2.** A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços da licitante ensejará a responsabilidade criminal, na forma da lei, sem prejuízo de outras providências nas demais esferas.

**10.3.3.** A licitante 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.

**10.3.4.** 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, quando assim se fizer necessário.

## 11. NATUREZA DO OBJETO (Art. 16, I)

**11.1.** 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”;

**11.2.** 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;

## 12. JUSTIFICATIVA PARA PARCELAMENTO DO OBJETO E FORMA DE ADJUDICAÇÃO (Art. 16, II e III)

**12.1.** 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.

**13. ADEQUAÇÃO ORÇAMENTÁRIA (Art. 16., V)**

| Id | Fonte (Programa / Ação) | Valor |
|---|---|---|
| 01 | **Fonte: FUNDO ESPECIAL DE REAPARELHAMENTO E MODERNIZAÇÃO DO JUDICIÁRIO - FERMOJU**<br>**Ação**: **20541**<br>**Tipo: SERVIÇO**<br>**Natureza: CUSTEIO**<br>**Exercício Financeiro (ano da despesa): 2023~2024** | **R$ 1.199.756,00** |
| | **TOTAL:** | **R$ 1.199.756,00** |

**13.1. Proposta de Preço**

**13.1.1. Organização da Proposta - AQSETIN2022015 – ANEXO IV – Modelo de Planilha de Formação de Preços**

**13.1.1.1.** A proposta deverá conter obrigatoriamente os seguintes elementos:

**13.1.1.2.** 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;

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

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

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

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

**13.1.1.7.** 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;

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

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

**13.2. Qualificação Técnica**

**13.2.1.** Para efeitos de comprovação da qualificação técnica, a licitante deverá enviar proposta comercial que contenha os Part Numbers (SKU) e quantidades descritas neste documento e que disponibilizará as licenças conforme prazo estabelecido;

**13.2.2.** A licitante deve disponibilizar, quando solicitado, todas as informações necessárias à comprovação de legitimidade do(s) atestado(s) apresentado(s) fornecendo, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual do TJCE e local em que foram prestados os serviços;

**13.2.3.** A CONTRATADA deverá apresentar, por ocasião da assinatura do contrato, no mínimo 1 (um) Gerente de Projetos, funcionário ou contratado da empresa, que será o líder e responsável pela entrega dos serviços de planejamento e implantação da Solução, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e

prazos estipulados no Edital. O Gerente de Projetos deve atender no mínimo aos seguintes requisitos:

**13.2.3.1.** Deve possuir escolaridade de nível superior completo;

**13.2.3.2.** Deve possuir certificação PMP – Project Management Professional do PMI – Project Management Institute ou possuir MBA – Master of Business Administration em Gerência de Projetos;

**13.2.4.** A CONTRATADA deverá apresentar, por ocasião da assinatura do contrato, no mínimo 1 (um) Responsável Técnico, funcionário ou contratado da empresa, que será o líder técnico, responsável pela prospecção, elaboração e implantação da Solução, além de responder por questões técnicas atinentes à Solução. Esse profissional deve possuir qualificação técnica comprovada, conforme requisitos descritos abaixo:

**13.2.4.1.** O Responsável Técnico deve possuir escolaridade de nível superior completo;

**13.2.4.2.** Deve possuir no mínimo certificação emitida pelo fabricante da principal solução proposta;

**13.2.5. DA HABILITAÇÃO**

**13.2.5.1.** Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

**a)** SICAF;

**b)** Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

**c)** Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

**d)** Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos – CADICON, mantidos pelo Tribunal de Contas da União - TCU;

**13.2.6.** Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c” e “d” acima pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoesapf.apps.tcu.gov.br/);

**13.2.7.** A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

**13.2.8.** Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

**13.2.9.** A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

**13.2.10.** O licitante será convocado para manifestação previamente à sua desclassificação.

**13.2.11.** Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

**13.2.12.** No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei

**13.2.13.** Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

**13.2.14.** Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

**13.2.15.** O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas.

**13.2.16.** É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

**13.2.17.** O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

**13.2.18.** Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos no Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 (duas) horas, sob pena de inabilitação.

**13.2.19.** Os documentos complementares a serem requisitados e apresentados não poderão ser os já exigidos para fins de habilitação no instrumento convocatório. Em outras palavras, não se trata de uma segunda oportunidade para envio de documentos de habilitação. A diligência em questão permite, apenas, a solicitação de documentos outros para confirmação dos já apresentados, sendo exemplo a requisição de cópia de contrato de prestação de serviços que tenha embasado a emissão de atestado de capacidade técnica já apresentado.

**13.2.20.** Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante a apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

**13.2.21.** Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

**13.2.22.** Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

**13.2.23.** Serão aceitos registros de CNPJ de licitante matriz e filial com diferentes números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

**13.2.24.** Os licitantes deverão encaminhar, nos termos deste ETP, a documentação nos itens a seguir, para fins de habilitação.

**13.2.25. HABILITAÇÃO JURÍDICA:**

**13.2.25.1.** Em se tratando de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual – CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

**13.2.25.2.** No caso de sociedade empresária ou empresa individual de responsabilidade limitada – EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

**13.2.25.3.** Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

**13.2.25.4.** No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

**13.2.25.5.** Decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

**13.2.25.6.** Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

**13.2.26. REGULARIDADE FISCAL E TRABALHISTA:**

**13.2.26.1.** Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

**13.2.26.2.** Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita

**13.2.26.3.** Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

**13.2.26.4.** Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

**13.2.26.5.** Prova de inexistência de débitos inadimplidos, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

**13.2.26.6.** Prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

**13.2.26.7.** Prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

**13.2.26.8.** Caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

**13.2.27. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**

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

**13.2.27.2.** 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;

**13.2.27.3.** 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;

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

**13.2.27.5.** 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 |

**13.2.27.6.** 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:

## 14. VIGÊNCIA CONTRATUAL (Art. 16., VI)

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

**14.2.** Para o fornecimento da solução a ser adquirida por até 70 (setenta) dias corridos, conforme previsto na tabela de **Requisitos temporais**, item **2.2** neste **ETP**. A contar da data de assinatura do contrato.

**14.3.** 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.

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

## 15. APROVAÇÕES

Declaramos a viabilidade da contratação, conforme justificativa apresentada no item **5** e os benefícios esperados listados no item **5.6** deste Estudo Técnico Preliminar, considerando os resultados pretendidos e as metas a serem alcançadas especificadas no Documento de Oficialização da Demanda.

**Equipe de Planejamento da Contratação**

| | | |
|---|---|---|
| Adarildo de Brito Figueiredo – 8025<br>**Integrante Requisitante** | Heldir Sampaio Silva – 9630<br>**Integrante Técnico** | Fábio de Carvalho Leite – 9594<br>**Integrante Administrativo** |

Cristiano Henrique Lima de Carvalho – 5198
**Autoridade Competente da Área Administrativa, em substituição.**

**Fortaleza, 2 de novembro de 2022.**