PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

REGINALDO GARCIA DUPIM
FRANCISCO JONATHAN REBOUCAS MAIA
DANIEL NEY GOMES PINHEIRO
DIVANIA MARIA ALCANTARA SOARES

ESTUDOS TÉCNICOS PRELIMINARES

Solução que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseado em risco, dos ativos de TIC, com análise contínua e adaptável de riscos e confiança, a fim de manter a disponibilidade, integridade e confidencialidades das informações.

1 ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (ART.14)

1.1 Contextualização

A consolidação do PJe vem proporcionando grandes avanços para a prestação jurisdicional da Justiça do Trabalho. Com o processo judicial existindo e tramitando exclusivamente no meio eletrônico, a tecnologia da informação passou a ser totalmente responsável pela guarda, integridade e disponibilidade de todos os autos dos processos.

Assegurar a confidencialidade, disponibilidade e integridade destes dados requer pessoal qualificado, processos definidos e tecnologias específicas.

Recentemente, temos observado um aumento significativo de ataques virtuais contra órgãos públicos brasileiros. Essas ações envolvem furto ou sequestro de informações.

Em novembro de 2020, o Superior Tribunal de Justiça foi alvo do maior ataque cibernético já realizado a um órgão do Governo Brasileiro. Foram mais de 7 dias com todos os sistemas indisponíveis. O foco do ataque foi a infraestrutura do Datacenter do STJ. Ataque com consequência semelhante foi realizado no Tribunal de Justiça do Rio Grande do Sul, TJ/RS, no final de abril de 2021, mas o foco, dessa vez, foram as mais de 12.000 estações de trabalho do TJ/RS, conhecidas como endpoints. Em 2022, o TRT da 17ª Região permaneceu com seus principais recursos de TIC, incluindo o PJE, indisponíveis por duas semanas, também por consequência de um ataque de ransomware.

Focos diferentes, estragos semelhantes, modo de operação similar: ataques do tipo ransomware que exploram vulnerabilidades existentes.

O cenário é tão crítico que o CTIR GOV, Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, criou uma série de recomendações para que eventos análogos não ocorressem em outros Órgãos. O CNJ também encaminhou recomendações similares a todos os Tribunais.

Com o avanço da ousadia e das técnicas utilizadas pelos hackers para causarem prejuízos às instituições, há a necessidade de aprimorar os

processos e ampliar as medidas preventivas e proativas de segurança da informação. Nesse sentido, o CNJ publicou a Resolução nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Em prosseguimento, publicou a Portaria nº 162/2021, que aprova Protocolos e Manuais criados pela ENSEC-PJ.

Entre os documentos aprovados está o Manual de Referência de Proteção de Infraestruturas Críticas de TIC.

O manual é baseado em um conjunto de boas práticas denominado CIS Controls, versão 7.1. Conforme o manual, por meio da adoção dos controles propostos por ele, estima-se que cerca de 85% (oitenta e cinco por cento) dos principais ataques praticados poderiam ser evitados. Entre as recomendações propostas, há as que já estão implantadas, as que necessitam de alteração em processos para serem implantadas e aquelas que necessitam de aquisição de ferramentas especializadas. Assim, as práticas não implementadas no manual e que requerem uso de ferramentas especializadas constituem os principais requisitos técnicos dessa demanda de contratação.

Oportuno ressaltar que, conforme expresso no Art. 5 da Portaria nº 162/2021, a implementação das práticas previstas nos manuais é obrigatória a todo Poder Judiciário:

> "Art. 5º Os protocolos e manuais aprovados por este ato deverão ser implementados por todos os órgãos do Poder Judiciário, com exceção do Supremo Tribunal Federal." (grifei)

No mesmo contexto de segurança da informação, a norma ABNT NBR ISO/IEC 27002:2013 trata de recomendações práticas para a gestão da segurança da informação.

Para atender às determinações do CNJ e as recomendações da norma ABNT NBR ISO/IEC 27002:2013, faz-se necessário a ampliação das ferramentas hoje disponibilizadas à equipe de TI do Tribunal, especialmente nos campos de identificação e classificação de vulnerabilidades técnicas para prevenção e mitigação de ataques danosos com ransomwares. Essas ferramentas devem abranger os ativos de TIC do Datacenter e as as estações de trabalho (endpoints).

1.2 Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

Com a contratação de ferramentas especializadas em segurança da informação, pretende-se colocar o Tribunal em acordo com as recomendações constantes no Manual de Referência de Proteção de Infraestruturas Críticas de TIC, aprovado através da PORTARIA CNJ No 162/2021, e às recomendações constantes na norma ABNT NBR ISO/IEC 27002:2013, no campo de gerenciamento de vulnerabilidades técnicas, vejamos:

O que diz a ABNT NBR ISO/IEC 27002:2013:

> "**12.6 Gestão de vulnerabilidades técnicas**
>
> Objetivo: Prevenir a exploração de vulnerabilidades técnicas.
>
> **12.6.1 Gestão de vulnerabilidades técnicas**
>
> Controle
>
> Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.
>
> Diretrizes para implementação
>
> Um inventário completo e atualizado dos ativos de informação (ver 8) é um pré-requisito para uma gestão efetiva de vulnerabilidade técnica. Informação específica para o apoio à gestão de vulnerabilidade técnica inclui o fornecedor de software, o número da versão, o status atual de desenvolvimento (por exemplo, quais softwares estão instalados e em quais sistemas), e a(s) pessoa(s) na organização responsável (is) pelos softwares.
>
> Convém que seja tomada ação apropriada, no devido tempo, como resposta às potenciais vulnerabilidades técnicas identificadas. É recomendável que as seguintes diretrizes sejam seguidas para o estabelecimento de um processo de gestão efetivo de vulnerabilidades técnicas:
>
> a) convém que a organização defina e estabeleça as funções e responsabilidades associadas na gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a

avaliação de risco de vulnerabilidades, correções, acompanhamento dos ativos e qualquer responsabilidade de coordenação requerida;

b) convém que os recursos de informação a serem usados para identificar vulnerabilidades técnicas relevantes e para manter a conscientização sobre os mesmos sejam identificados para softwares e outras tecnologias (baseado na lista de inventário dos ativos, ver 8.1.1); convém que esses recursos de informação sejam mantidos atualizados com base nas mudanças no inventário de ativos, ou quando outros recursos novos ou úteis sejam encontrados;

c) convém que seja definido um prazo para a reação a notificações de potenciais vulnerabilidades técnicas relevantes;

d) uma vez que uma vulnerabilidade técnica potencial tenha sido identificada, convém que a organização avalie os riscos associados e as ações a serem tomadas; tais ações podem requerer o uso de emendas de correções (patches) nos sistemas vulneráveis e/ou a aplicação de outros controles;

e) dependendo da urgência exigida para tratar uma vulnerabilidade técnica, convém que a ação a ser tomada esteja em acordo com os controles relacionados com a gestão de mudanças (ver 12.1.2) ou que sejam seguidos os procedimentos de resposta a incidentes de segurança da informação (ver 16.1.5).

f) se uma correção é disponibilizada, convém que sejam avaliados os riscos associados à sua instalação (convém que os riscos associados à vulnerabilidade sejam comparados com os riscos de instalação da correção);

g) convém que as emendas (patches) sejam testadas e avaliadas antes de serem instaladas para assegurar a efetividade e que não tragam efeitos que não possam ser tolerados; quando não existir a disponibilidade de uma emenda de correção, convém considerar o uso de outros controles, como: 1) a desativação de serviços ou potencialidades relacionadas à vulnerabilidade; 2) a adaptação ou a agregação de controles de acesso, por exemplo firewalls nas fronteiras da rede (ver 13.1); 3) o aumento do monitoramento para detectar ou prevenir ataques reais; 4) o aumento da conscientização sobre a vulnerabilidade.

h) convém que seja mantido um registro de auditoria de todos os procedimentos realizados;

i) com a finalidade de assegurar a eficácia e a eficiência, convém que processo de gestão de vulnerabilidades técnicas seja monitorado e avaliado regularmente;

j) recomenda-se contemplar em primeiro lugar os sistemas com altos riscos;

k) convém que um processo de gestão de vulnerabilidade técnica eficaz esteja alinhado com as atividades de gestão de incidentes, para comunicar dados sobre as vulnerabilidades, às funções de resposta a incidentes e fornecer procedimentos técnicos no caso em que ocorra um incidente.

l) convém que seja definido um procedimento para contemplar a situação onde uma vulnerabilidade tenha sido identificada e não existam controles adequados. Nesta situação, convém que a organização avalie os riscos relativos à vulnerabilidade conhecida e defina correções e ações corretivas apropriadas."

O que diz o Manual de Referência para Proteção de Infraestruturas Críticas de TIC estabelecido no Anexo VI da Portaria nº 162/2021 do Conselho Nacional de Justiça:

"**8 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.

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.

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.

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.

3.5 Implantar ferramentas de atualização automatizada de software de forma a garantir que os softwares de terceiros em todos os equipamentos sejam utilizados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.

3.6 Utilizar um processo de classificação de riscos para priorizar a remediação de vulnerabilidades descobertas.

Assim os requisitos de negócio da solução são as diretrizes expostas acima.

As especificações dos requisitos funcionais e não funcionais para contratação da solução serão elaborados durante e confecção do termo de referência. Neste estudo preliminar os requisitos elencados acima são suficientes para identificação das possíveis soluções e coleta de preços.

1.3 Soluções Disponíveis no Mercado de TIC (Art. 14, I, a)

- Aquisição de licenças perpétuas de software para gerenciamento de vulnerabilidades, com ou sem serviços de suporte e manutenção;

- Contratação de licenças para uso temporário de software, usualmente chamada de “subscrição”, para gerenciamento de vulnerabilidades, com ou sem serviços de suporte e manutenção;

- Contratação de serviços de gerenciamento de vulnerabilidades;

1.4 Contratações Públicas Similares (Art. 14, I, b)

Referência	Endereços eletrônicos
MUNICÍPIO DE SALVADOR - SEC. MUN. DE INOVAÇÃO E TECNOLOGIA - Pregão: 06/2021 - Licitacoes-e: 901163;	https://www.licitacoes-e.com.br/aop/documentos/L-901163/EDITAL_PE_006-2021_SEMIT.PDF, acesso em 19/05/2022 às 12h16
TRIBUNAL REGIONAL ELEITORAL-PB - Pregão: 37/2020;	https://www.tre-pb.jus.br/transparencia-e-prestacao-de-contas/gestao-de-contratacoes/licitacoes/pregao-eletronico/arquivos/2020/tre-pb-pregao-eletronico-37-2020/rybena_pdf?file=https://www.tre-pb.jus.br/transparencia-e-prestacao-de-contas/gestao-de-contratacoes/licitacoes/pregao-eletronico/arquivos/2020/tre-pb-pregao-eletronico-37-2020/at_download/file, e, https://www.tre-pb.jus.br/transparencia-e-prestacao-de-contas/gestao-de-contratacoes/atas-de-registro-de-precos/arquivos/arp-2020/tre-pb-ata-de-registro-de-precos-n-o-100-2020/rybena_pdf?file=https://www.tre-pb.jus.br/transparencia-e-prestacao-de-contas/gestao-de-contratacoes/atas-de-registro-de-precos/arquivos/arp-2020/tre-pb-ata-de-registro-de-precos-n-o-100-2020/at_download/file, e, https://www.tre-pb.jus.br/transparencia-e-prestacao-de-contas/gestao-de-contratacoes/atas-de-registro-de-precos/arquivos/arp-2020/tre-pb-ata-de-registro-de-precos-n-o-101-2020/rybena_pdf?file=https://www.tre-pb.jus.br/transparencia-e-prestacao-de-contas/gestao-de-contratacoes/atas-de-registro-de-precos/arquivos/arp-2020/tre-pb-ata-de-registro-de-precos-n-o-101-2020/at_download/file acesso em 19/05/2022 às 12h15
AGÊNCIA ESPACIAL BRASILEIRA - Pregão Eletrônico 06/2020 - Comprasnet.	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=203001&modprp=5&numprp=62020, e, https://www.portaltransparencia.gov.br/contratos/33119760?ordenarPor=descricao&direcao=asc, acesso em 19/05/2022 às 14h40

MINISTÉRIO PÚBLICO DO DFT - Pregão 62/2020 - Comprasnet;	https://www.mpdft.mp.br/transparencia/arquivos/licitacoes/pregaoeletronico202062resultado.pdf http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=200009&modprp=5&numprp=622020, acesso às 15h
MINISTÉRIO DA JUSTIÇA - Pregão 14/2021 - Comprasnet;	https://contratos.comprasnet.gov.br/transparencia/contratos?orgao=%5B%2230000%22%5D&vigencia_inicio=%7B%22from%22%3A%222021-10-01%22%2C%22to%22%3A%222022-02-01%22%7D http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=200005&modprp=5&numprp=142021, acesso em 19/05/2022 às 14h50
MINISTÉRIO DA JUSTIÇA - Pregão 19/2021 - Comprasnet;	https://contratos.comprasnet.gov.br/transparencia/contratos?orgao=%5B%2230000%22%5D&vigencia_inicio=%7B%22from%22%3A%222021-10-01%22%2C%22to%22%3A%222022-02-01%22%7D http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=200005&modprp=5&numprp=192021, acesso em 25/05/2022 às 13h
DETRAN/RO - Pregão 09/2020 - Comprasnet;	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=926002&modprp=5&numprp=92020#, acesso em 25/05/2022 13h10
SENAI - CI - Pregão 222/2020 - Sistema FIEB;	https://compras.fieb.org.br/Portal/Mural.aspx?nNmTela=E, acesso em 19/05/2022 15h20 (necessário filtrar pelo terno "vulnerabilidade" no campo "objeto" da tela de pesquisa;
TRIBUNAL DE CONTAS DO ESTADO DE RORAIMA - Pregão nº 17/2021 - Comprasnet;	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=925458&modprp=5&numprp=172021, acesso em 25/05/2022 12h40

COORDENAÇÃO GERAL DE TELEMÁTICA-DPF/DF - Pregão nº 1/2021 - Comprasnet;	http://comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=200342&modprp=5&numprp=12021, e https://www.gov.br/pf/pt-br/assuntos/licitacoes/2021/distrito-federal/orgaos-centrais/dti/contratos/contrato-06-2021-dti-pf/contrato-06-21-sei_pf-19281666.pdf/view, acesso em 25/05/2022 12h30
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO - Pregão 4/2022 - Comprasnet;	http://www.comprasnet.gov.br/ConsultaLicitacoes/download/download_editais_detalhe.asp?coduasg=80003&modprp=5&numprp=42022, acesso em 26/05/2022 11h25
SUPREMO TRIBUNAL DE JUSTIÇA - Contrato 86/2018, vigência de 31/12/2018 até 30/12/2022.	https://sei.stj.jus.br/sei//documento_consulta_externa.php?id_acesso_externo=20468&id_documento=1668606&infra_hash=85e21553921e54aeef5a86bd322370b6, acesso em 19/05/2022 à 14h27
SANEAGO - Pregão 94/201;	https://www.saneago.com.br/olc/olc/OLC128ListarDocumentosLicitacao.zul?numeroProcesso=4122&anoProcesso=2021 e https://www.licitacoes-e.com.br/aop/consultar-detalhes-licitacao.aop (lic. 916551), acessos em 19/05/2022 às 15h35
PRODEB - Pregão 09/2020;	http://www.prodeb.ba.gov.br/Documentos%20jurdico/PE_009_2020.rar, e, https://www.transparencia.prodeb.ba.gov.br/sites/default/files/documentos/arquivos-contratos/2020-12/Contrato%2020-065-01%20%281%29.pdf , acesso em 25/05/2022 15h20

1.5 Outras Soluções Disponíveis (Art. 14, II, a)

Desenvolvimento interno:

A robustez da solução exigiria da SETIC um esforço de desenvolvimento imenso (muito tempo e muitas pessoas), portanto incompatível com as responsabilidades desta unidade, que em apertada síntese, é de prover a

sustentação dos serviços de TIC, equipamentos e sistemas disponibilizados ao público interno e externo, tais como estações de trabalho, rede local, internet, site institucional e os sistemas PJE, SIGEP, PROAD, entre tantos outros.

Software livre:

Em pesquisa realizada na internet identificamos 2(duas) soluções livres, o Greenbone Vulnerability Manager (GVM)[1] e Open SCAP[2].

O GVM possui versões pagas e uma gratuita[3], sendo uma das mais populares quanto consideradas no universo de softwares livres.

O OpenSCAP[4] é uma coleção de ferramentas de código aberto para implementar e cumprir o padrão SCAP (Security Content Automation Protocol) certificado pelo NIST (Instituto Nacional de Padrões e Tecnologia). O objetivo é padronizar certas questões relacionadas à segurança. Uma forma de automatizar, até certo ponto, a busca por vulnerabilidades[5], avaliando seus possíveis impactos, gerenciando-os e avaliando as políticas a serem adotadas.

Analisando a documentação de ambas a equipe técnica entendeu que o Greenbone teria melhores condições de atender à demanda do TRT7, assim, a versão gratuita do Greenbone foi instalada na infraestrutura de TIC do TRT7 com o objetivo de realizar uma prova de conceito e iniciar a execução de processo de gerenciamento de vulnerabilidades, sem custo.

---

[1] https://github.com/greenbone/,
https://greenbone.github.io/docs/background.html#gvm-architecture
[2] https://www.open-scap.org/getting-started/
[3] https://www.greenbone.net/en/product-comparison/
[4] https://www.open-scap.org/
https://www.linuxadictos.com/pt/openscap-herramientas-seguridad-linux.html
[5] https://www.open-scap.org/features/vulnerability-assessment/

Como base na experiência de uso e da leitura de documentação complementar [6], descrevemos abaixo alguns pontos positivos e negativos do GVM:

Pontos negativos:

- Pouco intuitivo, assim a implementação e uso é mais complexa e demorada;
- Mensagens de erro não são muito claras;
- Base conhecimento (feed) depende da comunidade e não há garantia de funcionamento ou do tempo para disponibilização de vulnerabilidades e exposições comuns é descoberta (CVE). Neste tópico cabe mencionar que o coração de uma solução de gerenciamento de vulnerabilidade é a cobertura de CVE´s existentes e a agilidade em que são inseridas na base.
- Não há procedimentos de backup ou recuperação, exigindo da equipe a implementação destes recursos;
- Não há suporte, assim, em caso de dúvidas ou erros, a única opção é esperar por respostas voluntárias de outros usuários;
- Atualização de versão exige nova compilação dos códigos fontes e migração manual dos dados;
- Cobertura de CVEs menor que a de ferramenta pagas, como por exemplo Nessus/Tenable[7];
- O Greenbone/OpenVAS faz scan da máquinas, mas não de aplicações web, ou do Active Directory (serviço de diretório do usado pelo TRT7), não tem um agente para execução local na máquina, requisitos importantes e presentes em ferramentas pagas;

---

[6] https://www.gartner.com/reviews/market/vulnerability-assessment/vendor/greenbonenetworks/product/greenbonevulnerabilitymanagement/review/view/3675360#sub-head

https://www.greenbone.net/en/feed-comparison/

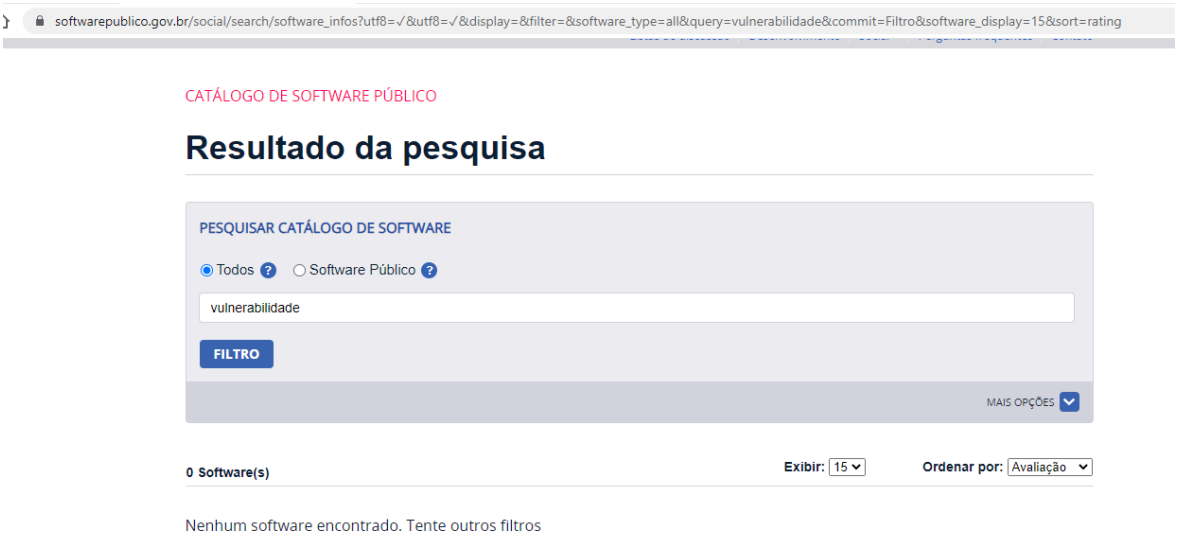
[7] https://www.comparitech.com/net-admin/nessus-vs-openvas

Pontos positivos:

- Comunidade forte;
- Código-fonte aberto;
- Custo zero (na versão aberta);
- Atualizado com frequência;
- Encontra vulnerabilidades comuns muito rapidamente;

1.6 Portal do Software Público Brasileiro (Art. 14, II, b)

Não há no Portal de Software Público Brasileiro solução que se possa atender essa demanda. Acesso ao portal https://softwarepublico.gov.br/social/search/software_infos realizado em 16.05.2022.



1.7 Alternativa no Mercado de TIC (Art. 14, II, c)

Não foram encontradas no mercado outras soluções, além das já consideradas no item 1.3 - soluções disponíveis.

1.8 Modelo Nacional de Interoperabilidade – MNI (Art. 14, II, d)

Não se aplica.

1.9 Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (Art. 14, II, e)

Não se aplica.

1.10 Modelo de Requisitos Moreq-Jus (Art. 14, II, f)

Não se aplica.

1.11 Análise Comparativa dos Custos das Soluções (Art. 14, III)

A possibilidade de licenciamento perpétuo nem será considerada na comparação de custos, em razão, como já justificado, de gerar dependência excessiva de um único fabricante ao longo de vários anos de renovações de suporte.

A tendência no mercado de TIC é contratação de subscrições, ou seja, cessão temporária de direito de uso de software.

Também não será realizada estimativa abrangente acerca da possibilidade de contratação de serviços, posto que, conforme já descrito, prestações de serviços vão onerar ainda mais a contratação, pois as ferramentas estão presentes da mesma forma, seja de responsabilidade da Contratada licenciá-las, seja da Contratante fornecer dentro do escopo dos serviços.

Dessa forma, a estimativa da contratação de cessão temporária de direito de uso de software será tratada no tópico “1.18 - Orçamento estimado”.

1.12 Escolha e Justificativa da Solução (Art. 14, IV)

Em linhas gerais, a conclusão da equipe é que embora o Greenbone (solução de software livre descrita no tópico 1.5) possa aprimorar a segurança da informação por meio da identificação das vulnerabilidades, não se configura a melhor alternativa em razão de não haver garantias de prazo para publicação de vulnerabilidades na base de descoberta, diferente das versões pagas que, normalmente, garantem a ação em 24 horas. Outro ponto fundamental é a ausência de facilidades como um painel de controle aprimorado para ganho de agilidade no processo de coleta, análise e enfrentamento das vulnerabilidades detectadas. Não menos importante, num cenário de ataques cibernéticos, cada vez mais frequentes e mais tecnicamente avançados, é garantir que a solução seja suportada por fornecedores capazes de aprimorar a solução na mesma velocidade. Assim, por todo o exposto, serão consideradas somente as soluções voltadas ao mercado corporativo, já amplamente testadas e utilizadas, que estejam melhor posicionadas em avaliações independentes.

Quanto às soluções de mercado descritas no tópico 1.3, a opção de licenciamento perpétuo será descartada pois exigiria renovações de suporte sempre com o mesmo fabricante, que poderia resultar altos custos pela impossibilidade da ampla concorrência, gerando na verdade dependência excessiva de um único produto. Já o modelo de subscrição resolve exatamente isso, a renovação será com o mesmo fabricante/produto enquanto o TRT7 achar que é mais vantajoso, podendo por ocasião das renovações cotar outros produtos para comparação de preços e, se for o caso, licitar novamente.

Outra possibilidade identificada é a contratação de serviços de gerenciamento de vulnerabilidades. Pode-se estabelecer o uso de ferramentas do Tribunal (atualmente não dispomos) ou que a Contratada as forneça dentro do escopo dos serviços. Dentro desse modelo pode ser contrato com quantitativo de serviço estimado e/ou banco de horas. Citamos como exemplo o Pregão

Eletrônico nº 67/2021 do Banco Central do Brasil - BCB[8]. Entendemos que, como as ferramentas são o coração dessa solução e o investimento é muito alto, a Contratada, na hipótese de ser a responsável pelo fornecimento, vai naturalmente embuti-las no faturamento mensal. Assim, entendemos que é melhor separar o custo dos serviços do custo de ferramentas. Em verdade, conforme a licitação do BCB, a contratação de serviços foca na aquisição de "expertise" para, além da identificação de ameaças pela varredura automatizada, atacar os ativos de TIC, visando aprimorar as linhas de defesa. Porém, essa é a modalidade mais cara, pois além das ferramentas, exige mão de obra super especializada, que atualmente possuem salários muito elevados, superando os R$ 25.000,00[9], e ainda incidindo as obrigações trabalhistas, previdenciárias e o lucro da empresa. Do ponto de vista de gestão, seria a melhor opção, já que o quadro de TIC do TRT7 não é mínimo exigido pelo CNJ na Resolução nº 370/2021. Porém, em razão do alto custo e de natureza continuada de mão de obra especializada, a equipe de planejamento entende que, neste momento, o ideal é a contratação de ferramenta de gerenciamento de vulnerabilidade para uso pela equipe do TRT7, o que não impediria, no futuro, a contratação de mão de obra de apoio operacional.

1.13 Descrição da Solução (Art. 14, IV, a)

Prover ao TRT7 solução que auxilie na prevenção e limitação da extensão de ataques cibernéticos, através do gerenciamento de vulnerabilidades, baseado em risco, dos ativos de tecnologia da informação, com análise contínua e adaptável de risco e confiança, a fim de manter a confidencialidade, a disponibilidade e a integridade das informações.

1.14 Alinhamento da Solução (Art. 14, IV, b)

A solução apresentada está alinhada às necessidades descritas neste documento e não há conflito com qualquer solução atualmente em produção no Tribunal.

---

[8] https://www.bcb.gov.br/Adm/Edital/pregaoe/DEMAP0672021/ecDEMAP0672021.pdf

[9] https://www.securityreport.com.br/overview/ciberseguranca-mercado-oferece-salarios-de-ate-r-26-mil-por-profissionais-especializados/#.YouRY6jMKM8

Quanto à estratégia, alinha-se:

-No contexto da gestão contínua de vulnerabilidades, à **Portaria CNJ nº 162/2021**[10], que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

-Ao Art. 26 da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), estabelecida pela **Resolução CNJ 396/2021**[11]**:**

> "Art. 26. Todos os órgãos do Poder Judiciário, à exceção do STF, deverão adotar e seguir, além dos Manuais de Referência para o gerenciamento, controle e padrões necessários ao aperfeiçoamento da segurança cibernética, o PPINC-PJ, que deverá contemplar um conjunto de diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível;..." (grifei)

-Ao objetivo estratégico "Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados", definido pela **Estratégia Nacional do Poder Judiciário, período 2021-2026**, instituída pela Resolução CNJ n. 325/2020[12].

-Ao objetivo estratégico "Aprimorar a Segurança da Informação e a Gestão de Dados", definido pela **Estratégia Nacional de TIC do Poder Judiciário, período 2021-2026,** instituída pela Resolução CNJ n. 370/2021[13].

Ao objetivo "Aprimorar a Governança de TIC e a proteção de dados", definido no **Planejamento Estratégico do TRT da 7ª**

[10] https://atos.cnj.jus.br/atos/detalhar/3982
[11] https://atos.cnj.jus.br/atos/detalhar/3975
[12] https://atos.cnj.jus.br/atos/detalhar/3365
[13] https://atos.cnj.jus.br/atos/detalhar/3706

Região, período 2021-2026, instituído pelo Ato TRT7.GP nº 64/2021[14].

Ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), biênio 2021-2022, pois foram incluídas duas ações no plano de contratação de TIC de 2022 (Anexo V do PDTIC) identificadas como "Solução de gerenciamento de vulnerabilidades - Licenciamento, treinamento, instalação" e "Solução de gerenciamento de vulnerabilidades - manutenção mensal", posto que foram aprovadas tais inclusões pelo Comitê de Governança de TIC 29/04/2022, conforme ata em anexo.

1.15 Benefícios Esperados (Art. 14, IV, c)

- Avaliar, de forma contínua, a existência de vulnerabilidades, reduzindo assim os riscos de ataques cibernéticos;
- Reduzir o risco de vazamento de dados (perda de confidencialidade);
- Reduzir o risco de alterações ou exclusões indevidas nos dados (perda da integridade);
- Reduzir o risco de paralisação prolongada dos serviços em razão de ataques cibernéticos (perda da disponibilidade);

1.16 Relação entre a Demanda Prevista e a Contratada (Art. 14, IV, d)

Inicialmente, cabe definir que o termo "servidores", neste contexto, será utilizado para descrever uma máquina (virtual ou física) que provê aos usuários internos ou externos algum serviço de TIC, tais como armazenamento de arquivos, sistemas de informação, autenticação de rede, portal web, integração de dados, entre tantos outros. É comum que um sistema de informação

[14] https://www.trt7.jus.br/pe/files/planejamento_estrategico/2021-2026/ATO_TRT7_GP_N_64_DE_04_DE_JUNHO_DE_2021_Plano_Estrategico_TRT7_2021_2026_2.pdf, acesso em 23/05/2022 12h

dependa de vários servidores, assim como um único servidor pode ofertar mais de um serviço.

A gestão de vulnerabilidade ocorre sobre os ativos de TIC, tais como desktops para os usuários (comumente chamados de endpoints), servidores dos mais diversos serviços e sistemas de TIC. Assim, a demanda prevista depende do inventário de "servidores" existentes nos dois data centers do TRT7, bem como do número de desktops. Assim, temos:

-**30** tipos de ativos de rede. O parque de ativos de rede (switches, por exemplo) é muito maior, mas considerando que esses equipamentos recebem poucas atualizações de software e é pouco provável a existência e o uso de vulnerabilidade, optou-se pelo licenciamento de 1(um) equipamento por tipo, assim, é possível identificar equipamentos vulneráveis com baixo custo, se comparado com licenciar todos.

-215 endereços internos e externos (FQDN´s), mas para a estimativa total será considerado **300** em função da dinamicidade e previsão de crescimento. A DITIC consultou em 18/05/2022 os registros de DNS[15] do TRT7 para verificar a quantidade de endereços de rede utilizados (cada endereço representa um sistema ou serviço, que pode exigir um ou mais servidores).

- 285 servidores linux e windows virtuais.

- 35 servidores físicos.

Diferentemente dos ativos de rede, servidores físicos e virtuais, bem como as aplicações, precisam ser licenciados na totalidade, já que a dinâmica de atualizações é muito grande, possuem configurações e softwares distintos, assim cada um possui/provê serviços específicos.

-2000 estações de trabalho e notebooks (endpoints). A Divisão de Suporte e Serviços de TIC reportou a existência de 1650 microcomputadores e 298 notebooks em uso, portanto 1948

[15] Essa relação não será inserida no processo administrativo pois expõe os endereços internos da rede de dados, que poderiam ser utilizados em ataques cibernéticos à infraestrutura de TIC do TRT7.

arredondado para 2000 para margem de erro. Quanto aos endpoints, embora exista uma padronização de sistema operacional e aplicações instaladas, é necessário licença para cada tombo devido:

- é a principal porta de entrada utilizada pelos hackers;
- vulnerabilidades são reportadas frequentemente;
- as atualizações automatizadas são demoradas e é comum ocorrerem falhas;
- robôs dos atacantes buscam na rede algum equipamento vulnerável, assim um único computador sem a atualização é rapidamente identificado;
- notebooks por não estarem “logados” não pegam as atualizações com regularidade;

- 500 containers de aplicação. Um container, no contexto de TIC, é um ambiente isolado. Um container contém um conjunto de processos que são executados a partir de uma imagem, imagem esta que fornece todos os arquivos necessários. A Divisão de Infraestrutura de TIC reportou a existência de 234 imagens apenas para o PJe, sendo 117 produção e 117 homologação. Como existe a tendência de ampliação do uso de imagens docker/kubernetes consideramos a demanda de 500 licenças no prazo de 5 anos.

1.17 Adequação do Ambiente (Art. 14, V, a, b, c, d, e, f)

Verificação da necessidade de adequação do ambiente físico ou técnico do TRT para o uso da solução.

Infraestrutura tecnológica:

Os requisitos de memória, processamento e armazenamento estão destacados abaixo:

RAM

22 GB (Log Correlation Events) + 8 GB (Nessus Scanner) + 16 GB (Nessus Manager) + 4 GB (NNM) + 16 GB (Web Application Scanning) + 2 GB (Container Scanner) = 68 GB de RAM

Processamento

8 cores (Log Correlation Events) + 4 Cores (Nessus Scanner) + 4 cores (Nessus Manager) + 2 cores (NNM) + 2 cores (Web Application Scanning) + 1 core (Container Scanner) = 21 cores de processamento

Disco

Em termos de disco, o espaço vai depender muito das funcionalidades habilitadas. Na página 78 do manual[16], para o menor número de clientes, há um cenário restrito que armazena dados por 180 dias e consome 1,8 TB de espaço.

Nessus Agent (cliente) = 1 GB + 2 cores

Sendo assim, hoje, temos recursos tecnológicos para receber a aplicação.

Infraestrutura elétrica:

Não se aplica.

Logística de implantação:

Por se tratar de solução de software, a logística se limita à definição de prazo e ações a serem cumpridas pela contratada descrita nas obrigações.

Espaço físico e mobiliário:

Não se aplica para a solução em si, mas somente para a capacitação. Na hipótese de ser realizada na modalidade presencial, o TRT possui equipamentos e ambiente adequado na Escola Judicial, devendo apenas agendar o uso dos mesmos. Na hipótese de ser realizada na modalidade telepresencial, o TRT também possui infraestrutura disponível e suficiente para a realização.

Impacto ambiental:

Não há.

16 https://docs.tenable.com/generalrequirements/Content/PDF/TenableGeneralRequirements.pdf, acesso em 02/06/2022 9h

Capacitação técnica:

A necessidade de capacitação técnica dos servidores que utilizarão o objeto a ser contratado foi considerada e incluída no escopo da demanda.

Capacitação para gestão e fiscalização do contrato:

Os servidores a serem indicados para gestão e fiscalização do contrato deverão possuir capacitação adequada para o desempenho dessas atividades.

1.18 Orçamento Estimado (Art. 14, II, g).

A equipe realizou pesquisas gerais na internet, no COMPRASNET[17] e no PAINEL DE PREÇOS[18] do Governo Federal.

Pesquisa de preços - Solução de Gerenciamento de Vulnerabilidades					
Órgão	**Referência**	**Licenciamento para solução de análise em dispositivos endpoint para 12 meses**	**Licenciamento para solução de análise para aplicações ou containers para 12 meses**	**Suporte técnico especializado mensal**	**Treinamento para 1 pessoa**
PRODEB*	Pregão: 9/2020	R$ 265,27	R$ 6.240,53		R$ 6.000,00
DPF*	UASG: 200342 Pregão: 01/2021 Comprasnet	R$ 138,70	R$ 12.400,00		R$ 10.200,00
SEMIT*	Pregão: 06/2021 Licitacoes-e: 901163	R$ 433,59	R$ 5.910,00		
MJ*	UASG: 200005 Pregão 19/2021 Comprasnet		R$ 8.681,25		

[17] https://www.gov.br/compras/pt-br/
[18] https://paineldeprecos.planejamento.gov.br/

TRE-PB	Pregão: 37/2020 Comprasnet	R$ 85,48	R$ 2.633,70		
AEB	UASG: 203001 Pregão: 06/2020 Comprasnet	R$ 387,12	R$ 387,12		R$ 8.804,17
MPDFT	UASG: 200009 Pregão: 62/2020 Comprasnet	R$ 344,70			
MJ	UASG: 200005 Pregão: 14/2021 Comprasnet	R$ 257,07			
DETRAN/RO	UASG: 926002 Pregão: 09/2020 Comprasnet	R$ 134,23			R$ 968,75
SENAI-CI	Pregão: 222/2020 Sistema FIEB	R$ 442,08			
SANEAGO	Pregão: 94/2021 Licitacoes-e: 916551	R$ 228,44			
STJ	Contrato 86/2018 (valor atualizado pelo INPC)	R$ 128,66			
TCE/RR	UASG: 925458 Pregão: 17/2021 Comprasnet	R$ 158,85	R$ 2.270,00		R$ 800,00
TRT8	UASG: 80003 Pregão: 17/2021 Comprasnet (valor ajustado para 12 meses)	R$ 290,60	R$ 240,80	R$ 10.000,00	R$ 8.600,00
Tenable Network	https://pt-br.tenable.com/buy Cotado com os limites de quantidades que da desconto da tela do e-commerce.	R$ 180,09	R$ 3.043,34		R$ 10.290,94

MÉDIA	**R$ 248,21**	**R$ 1.714,99**	**R$ 10.000,00**	**R$ 5.892,77**
*Valor do licenciamento para aplicações contratados pela PRODEB, DPF, SEMIT e MJ não foram utilizados na média por estarem muito acima dos demais				
MÉDIA CONSIDERANDO 60 MESES	**R$ 1.241,03**	**R$ 8.574,96**		

Conforme apurado na pesquisa demonstrada acima, verifica-se grande variação entre o menor e o maior valor em cada tipo de licenciamento, isso se deve a quatro fatores principais, que são:

- quantidade de licenças licitadas (economia por volume);
- presença ou ausência de serviços de instalação embutidos no custo do fornecimento das subscrições;
- presença ou ausência de suporte técnico especializado embutidos no custo de fornecimento das subscrições, que se difere da assistência técnica ofertada dentro do período de garantia;
- distribuição do custo entre os itens em mesmo lote;
- presença ou ausência de funcionalidades de scan de vulnerabilidades em aplicações web e containers, pois exige versões de topo de linha;

Assim, temos como resultado, considerando as quantidades necessárias ao TRT7 para estimativa de custo o seguinte:

Estimativa de custo			
Itens	Qtd	Valor unitário	Valor item
Licenciamento para solução de análise em dispositivos endpoint com garantia de 60 meses	1.645	R$ 1.241,03	R$ 2.041.488,66

Licenciamento para solução de análise para aplicações ou containers com garantia de 60 meses	800	R$ 8.574,96	R$ 6.859.969,07
Suporte técnico especializado mensal	60	R$ 10.000,00	R$ 600.000,00
Treinamento	9	R$ 5.892,77	R$ 53.034,94
Total Geral estimado para 5 anos (para todos os endpoints do TRT7 e todos as aplicações e containers identificados)			**R$ 9.554.492,67**

Para apuração da vantajosidade da ARP nº 5/2022 do TRT8, elaboramos a comparação abaixo, considerando os valores globais:

Comparação da Estimativa de Custo com a ARP nº 05/2022 do TRT8			
Itens	**Qtd TRT7**	**Valor unitário**	**Valor item**
1.Solução de gerenciamento de vulnerabilidades para FQDNs Externos, com serviços de implantação e garantia por 60 meses	120	R$ 1.150,00	R$ 138.000,00
2.Solução de gerenciamento de vulnerabilidades para FQDNs Internos, com serviços de implantação e garantia por 60 meses	180	R$ 1.115,00	R$ 200.700,00
3.Solução de gerenciamento de vulnerabilidades para imagens de aplicações em container, com serviços de implantação e garantia por 60 meses	500	R$ 1.204,00	R$ 602.000,00
4. Licenciamento para solução de análise em dispositivos endpoint para 60 meses	1.645	R$ 1.453,00	R$ 2.390.185,00

5. Suporte técnico especializado	60	R$ 10.000,00	R$ 600.000,00
6. Treinamento técnico da solução	9	R$ 8.600,00	R$ 77.400,00
Total Geral pela ARP 5/2022 - TRT8			**R$ 3.870.285,00**
Estimativa de custo pela pesquisa de preços			**R$ 9.554.492,67**
Redução			**-59,49%**

Percebe-se grande vantagem da utilização da ARP do TRT8, da qual o TRT7 é participante.

A principal explicação da expressiva redução em relação ao levantamento de preços é o volume licitado - economia de escala - já que envolveu a necessidade de 16(dezesseis) Tribunais do Trabalho. Percebe, ainda, comparando com a pesquisa de preços, que o fornecedor nivelou o preço das versões mais caras (que possibilita a gerência de vulnerabilidades em aplicações web, por exemplo) com o preço do custo do gerenciamento de vulnerabilidades em endpoints (versões de entrada). No resultado geral, considerando as quantidades envolvidas, os preços praticados na ARP em tela são amplamente vantajosos ao TRT7.

Contudo, considerando a capacidade operacional da SETIC para a implantação do processo de gerenciamento de vulnerabilidades, bem como visando priorizar os ativos de TIC que sustentam os sistemas de informação essenciais, após reunião interna de alinhamento (em 02/06/2022) optou-se pela compra inicial em volume inferior ao total registrado pelo TRT7 na ARP.

Em razão das peculiaridades das especificações técnicas e do volume licitado o produto que atende cada um dos itens é o mesmo, chamado Tenable.EP[19], ou seja, independente da quantidade de cada item o TRT7 receberá um único volume de licenças sem distinção do tipo de ativo de TIC. A necessidade real e imediata dos itens 1, 2 e 3 são 75, 140 e 330 respectivamente. Porém, como, na prática, não há distinção entre o produto que atende cada um dos itens,

[19] https://www.tenable.com/products/tenable-ep, acesso em 03/06/2022 9h

será solicitado na compra inicial a totalidade registrada para os itens 1, 2 e 3 pois os preços são inferiores ao do item 4, sendo que a quantidade excedente será descontada da necessidade do item 4 (endpoints), item mais caro da ARP.

Para os endpoints (item 4) a estratégia para a compra inicial foi a seguinte:

- licenciar 20% do total de microcomputadores e notebooks, portanto 400 (de 2000), de forma a permitir a gerência de vulnerabilidades por amostragem;
- licenciar 30 unidades para ativos de rede. Conforme já descrito, a quantidade de equipamentos existente é muito maior, mas será realizada varredura de vulnerabilidades em 1(um) equipamento de cada tipo.
- 1(uma) licença para cada servidor de rede físico (35) ou virtual (285);
- reduzir de 750 (400 + 30 + 35 + 285) para 495, em razão das 255 licenças excedentes dos itens 1, 2 e 3, gerando economia de R$ 69.485,00, pois reduz a compra inicial de R$ 1.856.820,00 para R$ 1.787.335,00.

Dessa forma a compra inicial será conforme a tabela abaixo:

COMPRA INICIAL				
Itens	**Qtd Registrada**	**Qtd TRT7**	**Valor unitário**	**Valor item**
1.Solução de gerenciamento de vulnerabilidades para FQDNs Externos, com serviços de implantação e garantia por 60 meses	120	120	R$ 1.150,00	R$ 138.000,00

2.Solução de gerenciamento de vulnerabilidades para FQDNs Internos, com serviços de implantação e garantia por 60 meses	180	180	R$ 1.115,00	R$ 200.700,00
3.Solução de gerenciamento de vulnerabilidades para imagens de aplicações em container, com serviços de implantação e garantia por 60 meses	500	500	R$ 1.204,00	R$ 602.000,00
4. Licenciamento para solução de análise em dispositivos endpoint para 60 meses	1.645	495	R$ 1.453,00	R$ 719.235,00
5. Suporte técnico especializado mensal	60	5	R$ 10.000,00	R$ 50.000,00
6. Treinamento técnico da solução	9	9	R$ 8.600,00	R$ 77.400,00
Total da compra inicial				**R$ 1.787.335,00**

2 SUSTENTAÇÃO DO CONTRATO (ART. 15)

2.1 Recursos Materiais e Humanos (Art. 15, I)

Recursos humanos:

Do Núcleo de Gestão de Segurança da Informação:

-01 Gestor do contrato;
-01 Servidor para uso da solução que também realizará a fiscalização técnica;

Da Divisão de Infraestrutura de TIC:

-01 Servidor para uso da solução;

Recursos materiais:

01 Servidor de rede físico ou virtual;

01 área de storage. Embora não seja possível determinar o espaço de disco exato necessário para rodar a solução, sabe-se que pela natureza da solução esse requisito não é grande o suficiente para justificar a compra de sistemas de armazenamento de dados, assim serão usados os equipamentos já existentes no TRT7.

2.2 Descontinuidade do Fornecimento (Art. 15, II)

Por se tratar de contratação de licença temporária de uso de software, o contrato deverá prever sanções em caso de interrupção contratual, com o objetivo de inibir essa prática.

Porém, na ocorrência de interrupção, será necessário conduzir nova licitação no menor tempo possível, já que os resultados almejados nestes serviços não estarão funcionando.

2.3 Transição Contratual (Art. 15, III, a, b, c, d, e)

Os serviços de TIC do TRT7 não dependem dessa solução para funcionamento, assim a transição contratual não requer cuidados especiais,

além daqueles típicos do planejamento anual de contratação para evitar a descontinuidade da solução de gerenciamento de vulnerabilidades.

2.4 Estratégia de Independência Tecnológica (Art. 15, IV, a, b)

A solução desenhada não gera qualquer dependência da tecnologia ou do fornecedor, podendo ser substituídos, caso necessário.

3 ESTRATÉGIA PARA A CONTRATAÇÃO (ART. 16)

3.1 Natureza do Objeto (Art. 16, I)

Apesar da robustez dos elementos que compõem essa demanda, as características são comuns no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos. O objeto é predominantemente de cessão temporária de licenças de software, incluindo serviço de suporte de natureza continuada, portanto, deverá se estender por mais de um exercício financeiro

No termo de referência serão incluídos critérios de qualificação econômico-financeira, por se tratarem de serviços continuados.

Cabe destacar que o objeto ora em análise é de interesse de toda Justiça do Trabalho, e por este motivo, o Tribunal Regional do Trabalho da 8ª Região conduziu processo licitatório tendo como participantes 16 TRT´s. O TRT8 informou em 10/11/2021 solicitando aos interessados que respondessem a intenção de registro de preços até 23/11/2021 (doc. 15).

Em duas semanas não foi possível a elaboração dos estudos técnicos preliminares devido a alta complexidade do objeto e o exíguo prazo para resposta. Por este motivo a equipe técnica, naquela oportunidade, realizou o que consideramos essencial, que foi o levantamento objetivo dos quantitativos necessários para contratação, conforme registrado no item “1.16 Relação entre a demanda prevista e a contratada”. Assim, após autorização da Diretora Geral (doc. 24), a IRP foi respondida.

3.2 Parcelamento do Objeto (Art. 16, II)

A hipótese de parcelar o objeto, como por exemplo, ter um produto/fabricante para gerência de vulnerabilidades nos endpoints, outro produto para o gerenciamento de vulnerabilidade em aplicações web, outro para aplicações em contêiner, exigiria duas ou mais capacitações, dois ou mais ambientes de controle, configuração e monitoramento. Hipótese muito mais dispendiosa para adquirir e, principalmente, sustentar. O que se pretende com a contratação é um console de gerenciamento centralizado que possa exibir os resultados das varreduras automatizadas, independente do tipo de ativo, registrar as ações de mitigação, de forma a manter continuamente o processo de gerenciamento de vulnerabilidade.

Assim, pelo exposto, a equipe entende que é inviável o parcelamento da solução.

Ademais, o parcelamento não ampliaria a concorrência, já que essas ferramentas são normalmente projetadas para atuarem nos mais diversos tipos de ativos de TIC, então separar por tipo, para efeito de concorrência, não teria resultado prático e possivelmente ampliaria o custo em função da redução de escala.

3.3 Adjudicação do Objeto (Art. 16, III)

De acordo com a impossibilidade de parcelamento do objeto, a adjudicação será somente para um fornecedor.

3.4 Modalidade e Tipo de Licitação (Art. 16, IV)

Apesar da robustez da solução, ela é ofertada por vários fornecedores e pode ser considerada comum no mercado de TIC. Assim, poderá ser realizada por Pregão Eletrônico por Menor Preço.

3.5 Classificação e Indicação Orçamentária (Art. 16, V)

Subscrição de Software (direito de uso por 60 meses):

Rubrica: 3.3.90.40.06 - LOCAÇÃO DE SOFTWARE .

Suporte técnico especializado (despesa continuada):

Rubrica: 3.3.90.40.07 - MANUTENÇÃO CORRETIVA / ADAPTATIVA E SUSTENTAÇÃO SOFTWARES.

Serviço de Treinamento:

Rubrica: 3.3.90.40.20 - TREINAMENTO / CAPACITAÇÃO EM TIC

3.6 Vigência da Prestação de Serviço (Art. 16, VI)

A vigência dos serviços de suporte técnico especializado será de 12 meses, renováveis até o limite legal.

A cessão dos direitos de uso dos softwares que compõem a solução deverá ser de 60(sessenta) meses, iniciados após o recebimento definitivo.

O prazo de assistência técnica deve ser incluído no prazo de vigência contratual, contados a partir do recebimento definitivo dos objetos, para fins de prestação dos serviços de assistência técnica.

As subscrições serão pagas em parcela única, por ser o modelo adotado pelo mercado. Já o serviço de suporte técnico especializado será pago mensalmente.

3.7 Indicação da Equipe de Apoio à Contratação (Art. 16, VII)

A equipe de planejamento foi nomeada pela Diretoria-Geral em 22.04.2022 (doc. 39), composta pelos seguintes membros:

Integrante Demandante: Reginaldo Garcia Dupim ;
Integrante Técnico: Daniel Ney Gomes Pinheiro ;
Integrante Administrativo: Divania Maria Alcantara Soares .

3.8 Indicação da Equipe de Gestão da Contratação (Art. 16, VIII)

Realizada a contratação, com a entrega dos produtos ou início dos serviços adquiridos, as responsabilidades de acompanhamento da execução contratual são assumidas pela **Equipe de Gestão da Contratação**, formada pelos seguintes servidores:

Gestor do Contrato

- Nome: Reginaldo Garcia Dupim
- E-mail: reginaldo.dupim@trt7.jus.br

Gestor Substituto do Contrato

- Nome: Robson Teixeira da Silva
- E-mail: robson.teixeira@trt7.jus.br

Fiscal Técnico

- Nome: Renan Vasconcelos Mazza
- E-mail: renanvm@trt7.jus.br

Fiscal Técnico Substituto

- Nome: Daniel Ney Gomes Pinheiro
- E-mail: danielngp@trt7.jus.br

4 ANÁLISE DE RISCOS

Risco:	Erro no dimensionamento das licenças e serviços a serem contratados	
Danos e impacto:	Caso maior: desperdício de recursos financeiros. Caso menor: não atingir os objetivos da contratação.	
Tipo de Ações	**Descrição da Ação**	**Responsável e Prazo**
Ação preventiva	-Emitir relatório no serviço de DNS para assegurar que a contagem de FQDN´s esteja de acordo com a realidade. Emitir relatório de endpoint ativos na solução de antivírus do TRT7;	DITIC / Antes da contratação

Ações de contingência	Repactuação contratual	DITIC / Sem prazo definido.

Risco:	Desempenho insuficiente da solução	
Danos e impacto:	Solução não prover nível adequado de proteção do ambiente tecnológico;	
Tipo de Ações	**Descrição da Ação**	**Responsável e Prazo**
Ação preventiva	Avaliar especificação técnica quanto a definição objetiva do desempenho esperado;	DITIC / Antes da licitação
Ação preventiva	Elaborar plano de implantação detalhado, para a correta configuração e parametrização da solução	DITIC e Contratada / Em até 30 dias após a contratação
Ações de contingência	Reunião de alinhamento; Revisão das configurações; Aplicação de sanções; Encerrar contrato; Nova contratação;	DITIC / Sob Demanda

Risco:	Falta de orçamento	
Danos e impacto:	Não contratar, impossibilidade de identificar e gerenciar continuamente as vulnerabilidades de forma adequada.	
Tipo de Ações	**Descrição da Ação**	**Responsável e Prazo**

Ação preventiva	-Aprovar demanda no CGTIC -Encaminhar estimativa de custo ao CSJT pleiteando os recursos necessários; -Incluir demanda de sustentação no plano de contratações de 2023	SETIC / Antes da licitação
Ações de contingência	-Reduzir o escopo de licenciamento; -Analisar as possibilidades de remanejamento do orçamento do TRT7	SETIC / Sob Demanda

Risco:	Identificação imprecisa da solução que atenda a demanda.	
Danos e impacto:	-Falhas no gerenciamento contínuo de vulnerabilidades de TIC. -Desperdício de recursos. -Não atingir os objetivos da contratação.	
Tipo de Ações	**Descrição da Ação**	**Responsável e Prazo**
Ação preventiva	-Verificar se as especificações técnicas estão alinhadas às práticas mais modernas na identificação e gerenciamento de vulnerabilidades; -Verificar o posicionamento do produto em avaliações realizadas por instituições independentes	NGSI/ Antes da licitação
Ações de contingência	Rescisão contratual e nova licitação	SETIC / Sob Demanda

5 ANEXOS

Não há.

6 ASSINATURAS

Considerando a demanda, a efetividade da solução, a capacidade de recepção do objeto, bem como sua instalação, configuração e uso pela SETIC, os integrantes da equipe de planejamento da contratação, descritos abaixo, declaram **a viabilidade** desta contratação.

EQUIPE DE PLANEJAMENTO		
Integrante Técnico	**Integrante Requisitante**	**Integrante Administrativo**
Daniel Ney Gomes Pi…	Reginaldo Garcia Dupim	Divania Maria Alcantar…
Fortaleza/CE, 06/06/2022		

DE ACORDO
Francisco Jonathan Reboucas Maia **DIRETOR** **SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO**
Fortaleza/CE, 06/06/2022