ESTUDO TÉCNICO PRELIMINAR

CARACTERIZAÇÃO DA DEMANDA

1. DESCRIÇÃO DA SOLUÇÃO A CONTRATAR.

Licença de uso do software para teste e análise estática de segurança de códigos em softwares e aplicações (sistemas informatizados) para plataforma Linux Red Hat 7.5 ou superior.

2. RESPONSÁVEIS PELO PLANEJAMENTO DA CONTRATAÇÃO.

A equipe de planejamento da contratação é composta pelos seguintes servidores, designados pela Portaria TSE 207/2019:

Integrante	Unidade	Email / Ramal
Lucas Ferreira de Lima (Integrante requisitante / STI)	SEPROP/COGTI/STI	lucas.lima@tse.jus.br / 8818
Thiago Melo Stuckert do Amaral (Integrante técnico / STI)	SEPROP/COGTI/STI	thiago.amaral@tse.jus.br / 8835
Carlos Eduardo Miranda Zottmann (Integrante técnico / STI)	COGTI/STI	carlos.zottmann@tse.jus.br / 9078
José Cipriano Neto (Integrante administrativo / SAD)	SECGA/CODAQ/SAD	jose.cipriano@tse.jus.br / 8078

3. CARACTERIZAÇÃO DA DEMANDA.

A Secretaria de Tecnologia da Informação (STI), por atribuição, desenvolve, mantém e evolui diversas soluções informatizadas (sistemas, softwares e aplicativos).

Essas soluções necessitam de mais garantias de segurança quanto às vulnerabilidades cada vez mais exploradas por ameaças internas e externas.

Com efeito, o cenário mundial de segurança cibernética comprova o incremento dos ataques direcionados às aplicações de informática. De acordo com um relatório de tendências sobre o assunto para 2019, elaborado pela empresa Radware[1], fabricante de

[1] The Trust Factor – Cybersecurity´s Role in Sustaining Business Momentum (https://www.radware.com/2018-ert-report-lpc-64459)

produtos de infraestrutura de segurança, o risco que mais preocupa as empresas neste ano, em todo o mundo, é justamente a questão de Vulnerabilidades em Aplicações (Application vulnerabilities), conforme ilustra o gráfico abaixo:

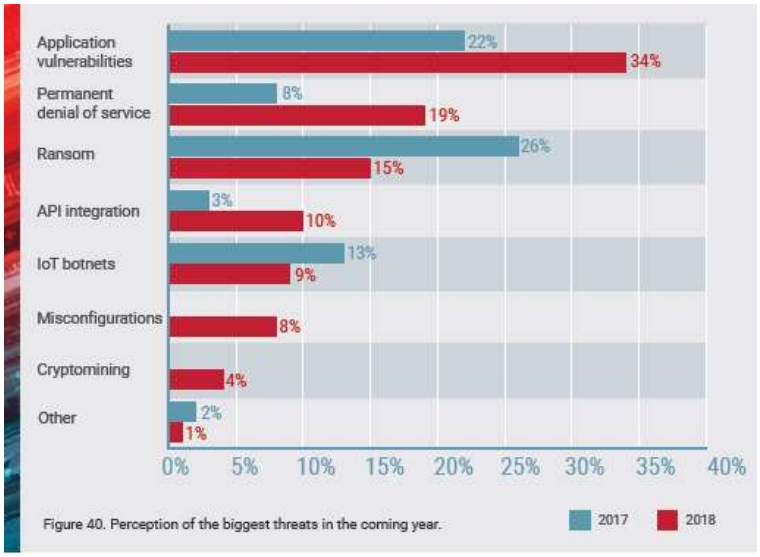


Figure 40. Perception of the biggest threats in the coming year.

A exploração de uma ou mais vulnerabilidades pode trazer sérias consequências à disponibilidade da prestação dos serviços que dependem desses sistemas, considerados de fundamental importância para o TSE, além da possibilidade de vazamento de dados. O mesmo estudo demonstra que esses são os dois principais objetivos dos ataques realizados em âmbito mundial, identificados no abaixo respectivamente como “Service disruption” e “Data theft”:

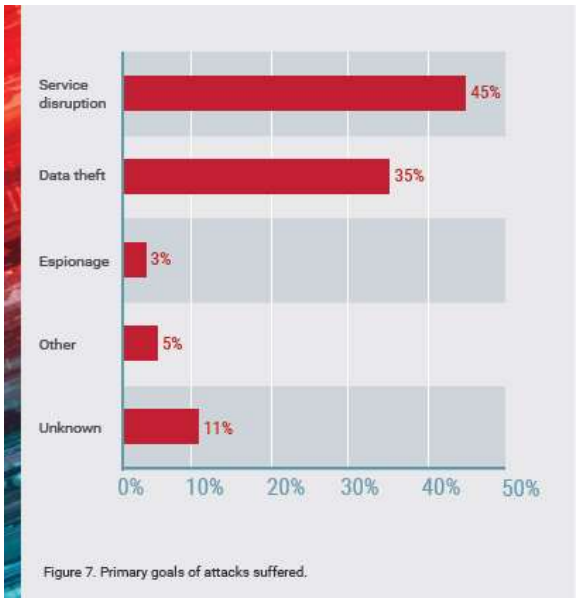


Figure 7. Primary goals of attacks suffered.

Já do ponto de vista financeiro, uma segunda análise, constante do mesmo relatório, indica que o custo gerado por um ataque bem sucedido, tanto sobre empresas que tenham entre 1.000 e 10.000 funcionários, quanto na vertical de governo, ambas categorias em

que o tribunal se encaixa, equivale a aproximadamente US$ 1.100.000,00 (cerca de R$ 4.000.000,00), conforme ilustram os gráficos abaixo:

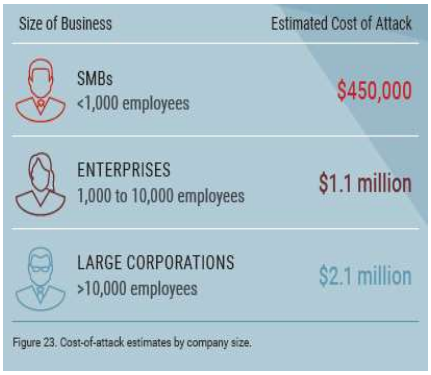


Figure 23. Cost-of-attack estimates by company size.

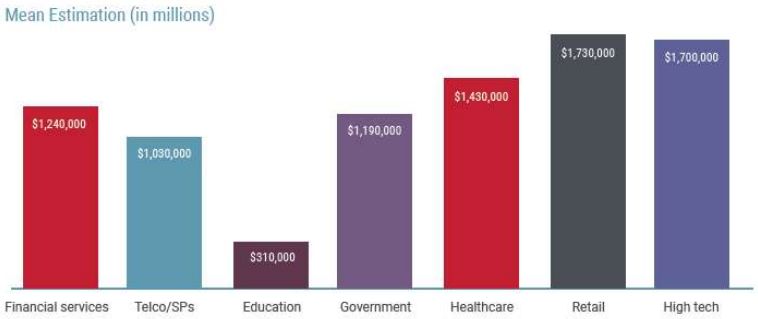


Figure 24. Estimated cost related to cyberattacks by vertical market.

Segundo o estudo, as perdas financeiras que podem ser quantificadas em decorrência de um ataque bem sucedido são de três naturezas distintas:

- Perda de receita;
- Custos não previstos;
- Queda no valor das ações.

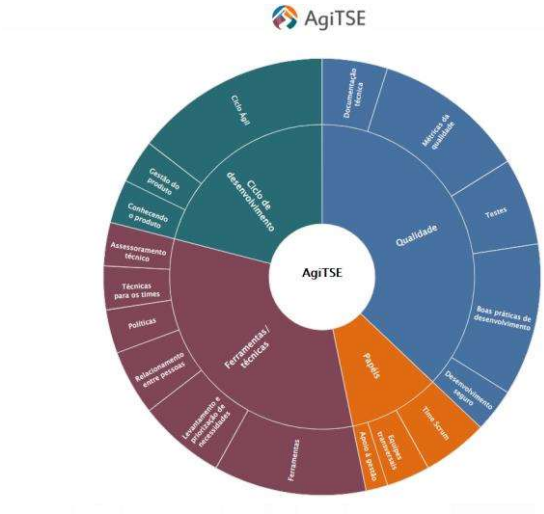
Embora perda de receita e queda no valor das ações não afetem órgãos públicos em geral, e o TSE em particular, certamente as atividades de reação a um ataque bem sucedido provocariam custos que não teriam sido previstos no orçamento anual.

Entretanto, no caso particular do tribunal, **devemos destacar o risco de imagem à credibilidade do órgão e do processo eleitoral em si, não abordados pelo estudo em questão, e para os quais não temos como estimar os custos**.

Em virtude do cenário acima descrito faz-se necessário que sejam adotadas medidas de segurança adicionais àquelas já em utilização no tribunal.

Nesse sentido, destacamos como indispensável a disciplina de Desenvolvimento Seguro de Software, parte integrante do Framework de desenvolvimento Ágil do TSE (AgiTSE)[2], que está sendo implantado na STI como padrão. A figura abaixo, que representa o AgiTSE, illustra que esta disciplina é um dos componentes do pilar de Qualidade:

[2] http://sticonhecimento.tse.jus.br/cogti/seprop/portal-da-agilidade/agitse



Ferramentas de análise estática de segurança de códigos em softwares e aplicações (conhecidas no mercado de TI como ferramentas SAST[3], objeto da aquisição pretendida) são essenciais para a implantação de desenvolvimento seguro, uma vez que proveem informações sobre vulnerabilidades que, em função da não utilização de boas práticas de codificação atualizadas, estejam sendo inseridas em seus desenvolvimentos. Tais ferramentas exibem alertas e oferecem informações e resultados necessários à mitigação dos problemas identificados, garantindo a redução das ameaças aos sistemas.

Com relação ao custo de correção de falhas de software, dentre as quais se enquadra a mitigação falhas de segurança, há diversos estudos publicados demonstrando seu crescimento exponencial ao longo do ciclo de vida do software, dentre os quais destacamos os seguintes:

- Os Impactos Econômicos de Infraestrutura Inadequada para Teste de Software[4] (tradução livre), publicado pelo National Institute of Standards and Technology, órgão do governo americano. Este relatório traz uma figura comparativa entre dois estudos referentes ao custo de reparação de defeitos em diferentes estágios do ciclo de vida de um produto:

Table 1-5. Relative Costs to Repair Defects when Found at Different Stages of the Life-Cycle

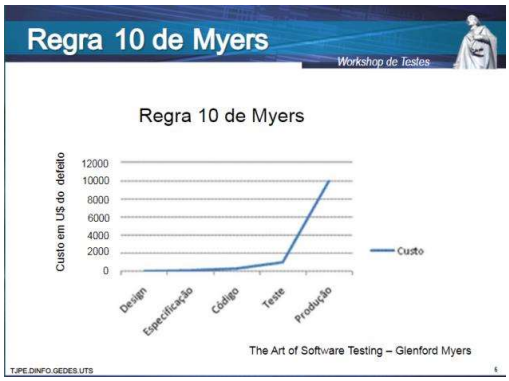
Life Cycle Stage	Baziuk (1995) Study Costs to Repair when Found	Boehm (1976) Study Costs to Repair when Found[a]
Requirements	1X[b]	0.2Y
Design		0.5Y
Coding		1.2Y
Unit Testing		
Integration Testing		
System Testing	90X	5Y
Installation Testing	90X-440X	15Y
Acceptance Testing	440X	
Operation and Maintenance	470X-880X[c]	

O estudo mais citado pela comunidade de desenvolvimento de software, exibido na última coluna, demonstra que o custo na fase de Testes de Instalação (Installation Testing) é 30 vezes maior do que o custo na fase inicial do projeto, equivalente ao Levantamento de Requisitos (Requirements).

[3] SAST: Static Application Security Testing

[4] The Economic Impacts of Inadequate Infrastructure for Software Testing (https://www.nist.gov/sites/default/files/documents/director/planning/report02-3.pdf)

- A Arte do Teste de Software (tradução livre), livro de Glenford Myers, cuja 3ª edição foi publicada em 2011, declara que o custo de correção de software em sua fase de utilização em produção é cerca de 10.000 vezes maior do que o na fase de projeto[5]:



Nesse sentido, destacamos que as ferramentas de análise estática de segurança de códigos em softwares e aplicações (SAST) podem ser utilizadas já na etapa de codificação dos softwares (podendo também ser utilizadas nas etapas seguintes), o que possibilita uma redução dos custos associados ao ciclo de desenvolvimento de software do tribunal.

3.1 TESTE PÚBLICO DE SEGURANÇA DE 2019.

Faz-se importante destacar, ainda, que, neste ano de 2019, será realizada mais uma edição do Teste Público de Segurança no ciclo de desenvolvimento dos sistemas de votação e apuração (TPS), conforme prevê a Resolução nº 23.444/2015.

Nesse contexto, faz parte do planejamento da Secretaria de Tecnologia da Informação a análise prévia de segurança dos códigos fonte, como parte do ciclo de desenvolvimento de tais sistemas, como um dos passos na direção do atendimento à recomendação da Comissão Avaliadora do TPS realizado em 2017 referente à certificação do processo seguro de desenvolvimento de software.

Considerando-se que o TPS de 2019 será realizado no mês de novembro, é importante que a presente contratação seja finalizada até o final do mês de agosto, ou, no mais tardar no mês de setembro, de forma a viabilizar a sua utilização tempestiva.

4. PREVISÃO ORÇAMENTÁRIA.

A aquisição ora pretendida encontra-se prevista na Proposta Orçamentária de 2019. Entretanto, conforme indicado no item 14 deste documento, propõe-se a utilização do Sistema de Registro de Preços de forma a viabilizar a contratação parcelada de licenças conforme a adoção da disciplina de análise estática de vulnerabilidades em códigos fonte por parte das diferentes equipes de desenvolvimento.

Assim, não será indicado neste documento o detalhamento da previsão orçamentária.

[5] https://slideplayer.com.br/slide/1265755/

5. ALINHAMENTO ESTRATÉGICO.

A aquisição objeto deste estudo alinha-se ao seguinte plano setorial:

- Plano Diretor de TI (2015-2017)

  Cumpre destacar que o Plano Diretor de TI - 2015-2017 é o que vigora atualmente. Sua atualização para contemplar novo período encontra-se em elaboração. As Ações Fundamentais (AF) com os quais esta aquisição contribui são as seguintes:

  - AF.04: Planejar, prover insumos, documentar e executar testes nos sistemas eleitorais utilizados em todas as fases do processo eleitoral e respectivas integrações, com o objetivo de aprimorar a qualidade dos produtos (Objetivo 6);

  - AF.06: Ampliar a utilização de técnicas e ferramentas para análise de código, automatização na construção de código e detecção rápida de erros, a fim de garantir melhor qualidade do produto entregue (Objetivo 6);

  - AF.12: Aperfeiçoar os procedimentos de segurança nos testes de sistemas, considerando recomendações de entidades conveniadas quanto à segurança da informação, com o objetivo de garantir mais qualidade aos sistemas produzidos (Objetivo 6);

  - AF.20: Revisar e aprimorar continuamente a segurança e a resiliência dos sistemas eleitorais (Objetivo 2);

  - AF.31: Utilizar, nos sistemas e nos aplicativos, os padrões de identidade visual, plataforma tecnológica e arquitetura, promovendo, se for o caso, a convergência/adequação daqueles que estiverem em desacordo, bem como a uniformização e a redução de custos (Objetivo 5);

  - AF.44: Promover a adoção de testes automatizados, a fim de ampliar a sua cobertura e a qualidade dos softwares produzidos (Objetivo 6);

  - AF.69: Estabelecer critérios de qualidade dos produtos de TI desenvolvidos pela STI (Objetivo 5);

O Plano Diretor de Tecnologia da Informação (PDTI), por sua vez, contribui com o planejamento estratégico de TI da seguinte forma:

- Planejamento Estratégico de Tecnologia da Informação do TSE (PETI 2015-2020)

    - **Objetivo 2 –** Ampliar a segurança e a transparência do processo eleitoral por meio de soluções de TIC
        - **Indicador 2.1**: Percentual de iniciativas de TIC que visem à ampliação da segurança da informação no âmbito do processo eleitoral brasileiro.
    - **Objetivo 5 –** Aprimorar os processos de gestão de TIC e padrões tecnológicos
        - **Indicador 5.2**: Percentual de sistemas de informação aderentes aos padrões de arquitetura de *software* de referência da STI.
    - **Objetivo 6 –** Garantir a confiabilidade nos produtos e serviços de TIC
        - **Indicador 6.3**: Percentual de qualidade de desenvolvimento de *software*.

Por fim, a aquisição pretendida também se alinha com o Planejamento Estratégico Institucional, por meio de contribuições para os seguintes objetivos estratégicos:

- Planejamento Estratégico Institucional TSE (PEI 2018-2020)

    - ***Objetivo Estratégico: OE1 – Assegurar a legitimidade do processo eleitoral***
        - Iniciativas: 1.3 Iniciativa estratégica: garantir a segurança dos sistemas eleitorais informatizados.

Destacamos ainda o alinhamento com o planejamento formulado pelo Conselho Nacional de Justiça para o Poder Judiciário, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

- Resolução CNJ nº 211/2015

    - *"Art. 20.* ***Os sistemas de informação deverão atender a padrões de*** *desenvolvimento, suporte operacional,* ***segurança da informação****, gestão documental, interoperabilidade e outros que venham a ser recomendados pelo Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário, e aprovados pela Comissão Permanente de Tecnologia e Infraestrutura do Conselho Nacional de Justiça."*

6. REQUISITOS SOLUÇÃO PARA ATENDER A NECESSIDADE DA CONTRATAÇÃO.

6.1 Requisitos Mínimos da Solução:

Item	Necessidades	Subitem	Principais Funcionalidades/Exigências
1	Licença de uso do *software* para teste e análise estática de segurança de códigos em *softwares* e aplicações (sistemas informatizados) para plataforma Linux Red Hat 7.5 ou superior	1.1	Análise de códigos fonte escritos nas linguagens de programação adotadas pelo tribunal.
		1.2	Análise de bibliotecas “open source” utilizadas nos projetos de software do tribunal
		1.3	Integração com a ferramenta “Jenkins” (ambiente de integração contínua).
		1.4	Integração com a ferramenta “SonarQube” (ambiente de Análise de Qualidade de Software)
		1.5	Integração com o Ambiente de Desenvolvimento Integrado (IDE) utilizado pelo tribunal.
		1.6	Base de conhecimento que ofereça, aos desenvolvedores, sugestões de correção dos problemas encontrados.
		1.7	Possibilidade de elaboração de Relatórios e *“Dashboards”* que indiquem a situação de segurança de cada projeto analisado, bem como do portfólio de projetos.
2	Serviço de instalação e configuração da solução		Instalação e configuração da solução sobre a infraestrutura de virtualização, e sua integração com os ambientes de Integração Contínua, Análise de Qualidade de softwares e Ambiente de Desenvolvimento Integrado do tribunal
3	Repasse de conhecimento		Repasse de conhecimento sobre a solução e suas particularidades de instalação e utilização no TSE, para as equipes de administração de infraestrutura, administração da solução adquirida, e equipes de desenvolvimento

4	Operação assistida		Acompanhamento técnico por parte da contratada ou do fabricante da solução fornecida, para viabilizar a internalização da solução pelo TSE de forma mais rápida e eficiente.

6.2 Requisitos de Sustentabilidade:

Serão aplicáveis à presente contratação os seguintes requisitos de sustentabilidade.

a) A solução de software objeto da aquisição a ser contratada, bem como sua documentação, deverá ser fornecida ao tribunal por meio de *"download"* a partir do sítio internet do fabricante, de forma a evitar o fornecimento desnecessário de recursos materiais;

b) Como condição prévia à assinatura do contrato e durante toda a vigência contratual, sob pena de rescisão, a contratada não deve possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTPS/MMIRDH Nº 4/2016, além de não ter sido condenada, a contratada ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta ao que está previsto no art. 1° e no art. 170 da Constituição da República, no art. 149 do Código Penal Brasileiro, no Decreto n° 5.017/2004 (decreto que promulga o Protocolo de Palermo) e nas Convenções da OIT nº 29 e nº 105;

- A comprovação de atendimento a esses critérios pode ser realizada por meio da verificação do nome da empresa em "lista suja" de empregadores flagrados explorando trabalhadores em condições análogas às de escravo emitida pela Secretaria do Trabalho do Ministério da Economia, atualizada periodicamente em seu sítio eletrônico (http://trabalho.gov.br/fiscalizacao-combate-trabalho-escravo). Para verificação sobre condenações, deve ser apresentada a Certidão Judicial de Distribuição, informalmente conhecida como "nada consta" ou "certidão negativa", da Justiça Federal, para a contratada e para seus dirigentes.

c) Em relação às condições de trabalho, a empresa contratada deve dar atendimento às normas regulamentadoras expedidas pelo então MTE quanto à Segurança e à Medicina do Trabalho, como elaborar e implementar o Programa de Controle Médico de Saúde Ocupacional (PCMSO), regulamentado pela NR 7, com o objetivo de promoção e preservação da saúde do conjunto de seus trabalhadores.

d) No que concerne à valorização do capital humano, devem ser garantidas a inserção e a inclusão de pessoas com deficiências em todas as esferas sociais e de trabalho. Caso a contratada seja empresa com cem ou mais empregados, ela deve atender ao disposto no art. 93 da Lei nº 8.213/91, no qual se determina que esse tipo de empresa está obrigada a preencher de 2% a 5% dos seus cargos com beneficiários reabilitados ou com pessoas com deficiência habilitadas na seguinte proporção:

I - até 200 empregados.....2%;

II - de 201 a 500.....3%;

III - de 501 a 1.000.....4%;

IV - de 1.001 em diante. .....5%.

7. LEVANTAMENTO DAS SOLUÇÕES DISPONÍVEIS NO MERCADO.

7.1 Soluções Técnicas disponíveis no mercado

O mercado de soluções do tipo de software que se pretende contratar é bastante amplo, oferecendo diversas soluções, tanto desenvolvidas e disponibilizadas sob os conceitos de software livre ou software gratuito, como soluções desenvolvidas e disponibilizadas como softwares comerciais.

A entidade OWASP (Open Web Aplication Security Project), internacionalmente reconhecida como uma das principais fontes de conhecimento e de divulgação de boas práticas referentes ao assunto, disponibiliza em seu site[6] uma relação não exaustiva de tais produtos, contemplando 19 soluções livres ou gratuitas, e 29 soluções comerciais.

Dentre as soluções livres ou gratuitas destacamos o SonarQube e o FindSecBugs, atualmente utilizados em conjunto pelas unidades de desenvolvimento de software no TSE para a função de análise estática de segurança de códigos.

Com relação às alternativas comerciais, em que pese o fato de que o rol de soluções ofertados no mercado nacional apresente algumas diferenças em comparação à relação apresentada no site da OWASP, a quantidade de soluções disponíveis inviabiliza a efetiva análise de todas elas, em função do tempo, esforço e capacidade computacional necessários a avaliação de cada ferramenta, e a disponibilidade desses recursos na STI.

Adicionalmente, há soluções comerciais cujo modelo de comercialização é baseado na instalação das ferramentas na infraestrutura computacional do cliente, e outras que já contemplam sua utilização em modelo de nuvem, isto é, instaladas em infraestrutura computacional de responsabilidade do próprio fornecedor, acessada por meio da Internet.

Tendo em vista que o TSE ainda não regulamentou a utilização de produtos de computação em nuvem, de tal forma que os riscos e submissão de código fonte a soluções desta natureza, as alternativas baseadas neste modelo foram descartadas.

Assim, foram realizadas Provas de Conceito com três produtos distintos, selecionados dentre aqueles de destaque no mercado internacional[7], a partir de uma análise inicial de suas documentações, mostraram potencial de atendimento às necessidades do tribunal. As ferramentas analisadas foram as seguintes:

[6] https://www.owasp.org/index.php/Source_Code_Analysis_Tools

[7] https://www.gartner.com/doc/reprints?id=1-4RBB1XO&ct=180216&st=sb

- Checkmarks CxSAST
- Fortify Static Code Analyzer
- BugScout

7.2 Modalidades de Contratação

Com relação às modalidades de contratação para este tipo de solução, observou-se que são três as disponíveis no mercado:

- Aquisição da solução, contemplando suporte técnico remoto pelo fabricante e atualização de versões durante a validade da licença de uso;
- Subscrição da solução, modalidade em que não há a aquisição das licenças de software, mas somente a contratação de seu direito de utilização por tempo determinado, também acompanhado de suporte técnico remoto pelo fabricante e atualização de versões durante a validade da licença de uso.
- Utilização em modelo de nuvem: não se cogita utilização da solução baseada na utilização da ferramenta em nuvem pública, em razão da ausência de regulamentação do TSE sobre o tema, conforme exposto no item 7.1, sobretudo pela criticidade das informações submetidas às análises de segurança.

Durante a pesquisa de preços realizada com base exclusivamente em preços publicamente disponíveis a partir de resultados de licitações, identificamos apenas exemplos de contratações realizadas no modelo de subscrição[8].

Entretanto, em razão da solicitação do Gabinete da Diretoria Geral, contida no documento 1065764, referente à demonstração do custo/benefício das diferentes opções, solicitamos, a um dos fornecedores da mesma solução contemplada no Pregão nº 12/2018 do Exército Brasileiro, cotações baseadas tanto no modelo de aquisição quanto no modelo de subscrição, inseridas neste processo como documentos XXXXX e YYYYY, a partir dos quais elaboramos a tabela abaixo:

	Aquisição (A)		**Subscrição (S)**		**Variação (A – S)**	
	Preço Anual	Acumulado	Preço Anual	Acumulado	Nominal	%
ANO 1	1.561.074,35	1.561.074,35	1.176.588,54	1.176.588,54	384.485,81	24,62
ANO 2	390.268,60	1.951.342,95	1.176.588,54	2.353.177,08	-401.834,13	-17,07
ANO 3	390.268,60	2.341.611,55	1.176.588,54	3.529.765,62	-1.188.154,07	-33,66
ANO 4	390.268,60	2.731.880,15	1.176.588,54	4.706.354,16	-1.974.474,01	-41,95

Com efeito, observa-se que os custos referentes ao primeiro ano de utilização da solução são superiores no cenário de aquisição em relação ao cenário de subscrição, conforme havia sido citado na versão anterior destes Estudos Técnicos Preliminares.

[8] Pregão nº 12/2018 do Exército Brasileiro (Documentos 1008966, 1008982 e 1008984) e Ata de Registro de Preços nº 1/2018 da Imprensa Nacional (Documento 1009004)

Entretanto, a partir do segundo ano de utilização o cenário se inverte, de forma tal que os custos relativos à aquisição no primeiro ano e renovação dos direitos de renovação e suporte nos anos subsequentes se tornam inferiores ao cenário da renovação da subscrição.

8. VANTAGENS E DESVANTAGENS DE CADA SOLUÇÃO

8.1 Continuidade da utilização de solução gratuita

- Vantagens:
  - Inexistência de custos de aquisição
- Desvantagens
  - Capacidade de análise de problemas de segurança apenas em código-fonte desenvolvido na linguagem Java[9];
  - Menor capacidade de detecção de vulnerabilidades no código-fonte;
  - Menor qualidade das Bases de conhecimento e formas de orientação quanto à solução das vulnerabilidades encontradas;
  - Inexistência de acoplamento com Ambientes de Desenvolvimento Integrado (IDEs), o que possibilitaria que os desenvolvedores tomassem conhecimento dos problemas de segurança ainda em tempo de construção inicial dos softwares;
  - Incerteza quanto à política de disponibilização de atualizações dos conteúdos de segurança utilizados para a detecção de vulnerabilidades (uma vez que os conteúdos de segurança dependem de contribuição voluntária da comunidade de desenvolvedores do produto);
  - Inexistência de suporte técnico comercial.

8.2 Aquisição de solução comercial:

- Vantagens:
  - Capacidade de análise de problemas de segurança nas demais linguagens de programação utilizadas pelo TSE;
  - Maior capacidade de detecção de vulnerabilidades no código-fonte;
  - Maior qualidade das Bases de conhecimento e formas de orientação quanto à solução das vulnerabilidades encontradas;
  - Funcionalidade de acoplamento com Ambientes de Desenvolvimento Integrado (IDEs), o que possibilitaria que os desenvolvedores tomassem conhecimento dos problemas de segurança ainda em tempo de construção inicial dos softwares;
  - Política definida de disponibilização de atualizações dos conteúdos de segurança utilizados para a detecção de vulnerabilidades;
  - Disponibilidade de suporte técnico comercial;
  - Custos de propriedade mais baixos a partir do segundo ano, em comparação à opção de subscrição.
- Desvantagens:

[9] https://github.com/find-sec-bugs/find-sec-bugs/releases/tag/version-1.9.0

- Custos de propriedade mais altos durante o primeiro ano, em comparação à opção de subscrição.

8.3 Subscrição de solução comercial:

- Vantagens:
  - Capacidade de análise de problemas de segurança nas demais linguagens de programação utilizadas pelo TSE;
  - Maior capacidade de detecção de vulnerabilidades no código-fonte;
  - Maior qualidade das Bases de conhecimento e formas de orientação quanto à solução das vulnerabilidades encontradas;
  - Funcionalidade de acoplamento com Ambientes de Desenvolvimento Integrado (IDEs), o que possibilitaria que os desenvolvedores tomassem conhecimento dos problemas de segurança ainda em tempo de construção inicial dos softwares;
  - Política definida de disponibilização de atualizações dos conteúdos de segurança utilizados para a detecção de vulnerabilidades;
  - Disponibilidade de suporte técnico comercial;
  - Custos de propriedade mais baixos durante o primeiro ano, em comparação à opção de aquisição.
- Desvantagens:
  - Custos de propriedade mais altos a partir do segundo ano, em comparação à opção de aquisição.

9. ESCOLHA DA SOLUÇÃO.

A equipe de planejamento da contratação entende que a melhor opção para esta primeira contratação de software de análise estática de segurança em código-fonte (SAST) seja baseada em períodos de vigência não muito longos, uma vez que esta disciplina está em processo de implantação, o que exigirá um maior esforço de aprendizagem e de implantação e que poderá, ao longo do tempo, evidenciar novos requisitos de análise e consequentemente novas funcionalidades a serem utilizadas, eventualmente demandando ferramentas mais completas do que a que se pretende contratar.

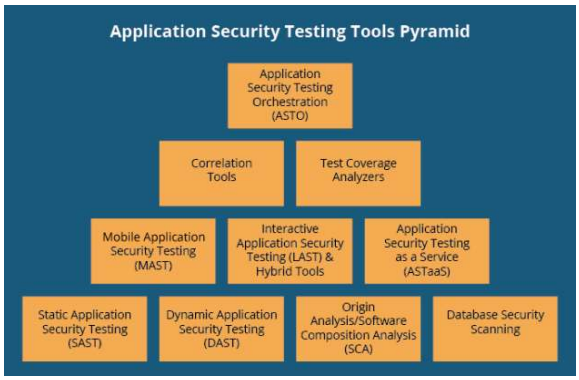
Com efeito, artigos técnicos especializados evidenciam essa questão, a exemplo do artigo *"10 Types of Application Security Testing Tools: When and How to Use Them"*[10], publicado pelo Software Engineering Institute da Universidade Carnegie Mellon, dos Estados Unidos.

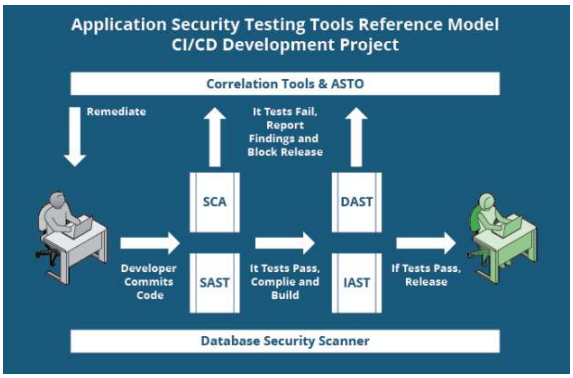
O artigo apresenta diversos tipos de ferramentas de análise de segurança em aplicações, para diferentes cenários de testes, tais como SAST, DAST, SCA, IAST e MAST (a explanação das siglas não se faz necessária neste contexto), e, em seu tópico "Selecting Testing Tool Types" (Selecionando tipos de ferramentas de testes), informa que:

[10] https://insights.sei.cmu.edu/sei_blog/2018/07/10-types-of-application-security-testing-tools-when-and-how-to-use-them.html

- *"Se a aplicação é escrita internamente ou se a equipe tem acesso ao código fonte, um bom ponto de partida é a execução de uma ferramenta análise de vulnerabilidade estática de código fonte (SAST) e verificar problemas de código e aderência a padrões de codificação. De fato, ferramentas SAST são o ponto inicial mais comum para análise de código."*[11]

Os quadros abaixo, extraídos do mesmo artigo, evidenciam este papel inicial das ferramentas SAST no ciclo de análise de segurança de aplicações:





Observa-se que tanto na Pirâmide de Ferramentas de Testes de Segurança em Aplicações (quadro da esquerda) quanto no Modelo de Referência do Ciclo de Testes de Segurança em Aplicações (quadro da direita) as ferramentas de análise estática de segurança (SAST) são posicionadas nos respectivos estágios iniciais.

Justificada a opção pela aquisição de solução comercial de análise estática de segurança (SAST), resta a opção pelo modelo de contratação.

Em uma primeira análise o modelo de subscrição apresenta menor custo inicial, inferior em R$ 384.485,81 em comparação ao modelo de aquisição, o que equivale a aproximadamente 24%.

Entretanto, já no segundo ano de utilização da solução o cenário se inverte, e o custo acumulado ao longo dos dois anos se revela inferior em R$ 401.834,13, ou aproximadamente 17%, consolidando-se como opção mais econômica nos períodos subsequentes.

Em razão do esforço de aprendizagem e de implantação previstos, não é desprezível a probabilidade de que a maturidade da disciplina de análise estática de segurança em código-fonte seja atingida somente no segundo ou terceiro ano de utilização.

Desta forma, considerando-se os valores e o tempo de maturidade envolvidos, entende-se que o cenário de aquisição da solução com direito a atualização de versões e suporte técnico remoto pelo período de 36 meses tem maior probabilidade de proporcionar maior economia ao longo do amadurecimento da disciplina.

Assim, a solução escolhida é a licitação para a aquisição de solução comercial, em função da maior qualidade destas em relação às soluções livres ou gratuitas, com base em

[11] Tradução livre

especificações técnicas que permitam a ampla competitividade, ao mesmo tempo em que garantam o atendimento às necessidades do tribunal.

10. ESTRATÉGIA PARA A CONTRATAÇÃO.

A solução escolhida apresenta as seguintes características:

Natureza	Aquisição de software com Prestação de Serviços (mão de obra não exclusiva).
Características comuns e usualmente encontradas no mercado	Sim.
Subcontratação	O objeto deve ser executado única e exclusivamente pela licitante contratada, haja vista que o mercado dispõe de diversas empresas aptas a executar integralmente o objeto a ser licitado.
Consórcio	Não é necessária a previsão de participação de empresas de forma consorciada, visto que no mercado encontram-se várias empresas aptas a fornecer o objeto de forma isolada.
Contrato atual vigente	Não.
Legislação aplicável à licitação	• Decreto nº 7.174/2010 - Bens e serviços de informática e automação.
Legislação aplicável ao objeto	Não há conhecimento de nenhuma legislação específica afeta ao objeto a ser contratado
Previsão de forma de contratação	Objeto a ser licitado (e.g. pregão, concorrência, tomada de preço, convite, concurso, leilão).
Haverá possibilidade de prorrogação do contrato?	Sim. A contratação trata de utilização de programas de informática (art. 57, IV, da Lei nº 8.666/93).
Prazo de garantia/validade que será exigido dos objetos contratados é usual de mercado?	Sim.
Análise da Divisibilidade da Solução	Não é possível parcelar o objeto uma vez que o produto a ser adquirido é composto por um único software, de natureza indivisível. Eventuais variações em torno da configuração de produtos de mesmo fornecedor são decorrentes do licenciamento para diferentes quantidades de usuários, projetos de software a serem avaliados, e quantidade de linhas de código que compõem tais projetos, que, entretanto, não permitem sua divisão em itens distintos. Adicionalmente, considerando-se que a aquisição será realizada sem a indicação de marca ou modelo, tem-se que os serviços complementares a serem contratados não podem ser vinculados previamente a nenhum produto específico, mas devem ser vinculados ao produto que venha a ser adquirido, de forma que a separação desses serviços em itens ou lotes distintos também se torna inviável.

11. RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE CADA ITEM.

A aquisição de ferramenta de análise estática de segurança de códigos em softwares e aplicações tem como objetivo final sua utilização por todas as equipes de desenvolvimento do tribunal, em projetos de software já existentes em ambiente de produção e nos novos projetos que vierem a ser desenvolvidos.

Entretanto, conforme indicado no item 14 deste documento, sua adoção deverá ser gradual, em função das alterações que serão introduzidas nas rotinas de trabalho das equipes citadas.

Ao final do projeto, sua utilização envolverá os seguintes números:

- 2 Coordenadorias da STI responsáveis pelo desenvolvimento de software;
- 12 Seções responsáveis pelo desenvolvimento de software;
- 4 administradores (equipes da SEPROP e de Segurança);
- 30 gestores de projetos de software (Chefes de Seção, Coordenadores, Secretário e Assessor);
- 180 desenvolvedores (ativos no ambiente GitLab em 2019);
- 200 projetos de software;

12. ESTIMATIVA DE PREÇOS PRELIMINAR.

A estimativa de preços abaixo apresentada ainda carece de maior detalhamento da especificação técnica, que somente será alcançada por ocasião da elaboração do Termo de Referência, bem como de maior representatividade em termos de fontes de informações de preços, uma vez que é baseada apenas no valor da proposta apresentada pela empresa Cipher.

Licitação por lote					
Lote	**Item**	**Descrição**	**Unidade de Fornecimento**	**Qtd.**	**Preço Estimado (R$)**
1	1	Aquisição de *software* para teste e análise estática de segurança de códigos em *softwares* e aplicações (sistemas informatizados)	Quantidade de Projetos de Software submetidos à solução	200	2.341.611,55
	2	Serviço de instalação e configuração da solução	Execução	1	236.762,23
	3	Repasse de conhecimento	Execução	1	
	4	Operação assistida	Execução	1	
				TOTAL	2.578.373,78

Em função das restrições de consulta que embasaram a presente estimativa, ressaltamos que a verificação do modelo mais vantajoso (aquisição ou subscrição) **deverá ser novamente realizada quando o Termo de Referência tiver sido finalizado**, contendo todas as especificações técnicas pertinentes à solução de software e aos serviços associados.

13. RESERVA DE 25% PARA ME/EPP NAS AQUISIÇÕES.

Em virtude da natureza indivisível do objeto, entende-se que seja inviável a adoção tal reserva.

14. APLICAÇÃO DA MARGEM DE PREFERÊNCIA OU DIREITO DE PREFERÊNCIA.

Atualmente não há legislação vigente que estabeleça margem ou direito de preferência para aquisições ou subscrições de software.

15. VIGÊNCIA DA PRESTAÇÃO DE SERVIÇO.

Os diferentes serviços relacionados no item 5 deste documento têm as seguintes previsões de duração de execução:

Item	Serviço	Vigência	Prorrogável
1	Aquisição de *software* para teste e análise estática de segurança de códigos em *softwares* e aplicações (sistemas informatizados) com direito a atualização de versão e suporte técnico remoto.	36 meses	Não
2	Serviço de instalação e configuração da solução	1 mês	Não
3	Repasse de conhecimento	5 dias úteis	Não
4	Operação assistida	10 dias úteis	Não

16. UTILIZAÇÃO DO SISTEMA DE REGISTRO DE PREÇO.

Objetiva-se a contratação parcelada uma vez que a adoção da solução no âmbito do TSE deverá ocorrer de forma gradativa, uma vez que trará modificação nas rotinas adotadas pelas diversas unidades responsáveis pelo desenvolvimento de software.

Atualmente cerca de 50 projetos de software do TSE estão sendo submetidos à análise estática de código por meio da solução gratuita SonarQube+FindSecBugs.

O planejamento de implantação da ferramenta prevê sua adoção inicial para estes 50 projetos, com inclusão de novos projetos em fases distintas. Tem-se como objetivo incluir todos os 164 projetos que hoje já obedecem às políticas de arquitetura de sistemas

que permitam sua inclusão no ambiente de integração contínua, e é prevista ainda a possibilidade de adequação de novos projetos para esta forma de trabalho, com potencial de alcance de 200 projetos ao todo.

Assim, indicamos a utilização do Sistema de Registro de Preços (SRP) de forma a viabilizar esta implantação em fases, de forma que sejam adquiridas novas licenças da solução de forma sincronizada com a inclusão de novos projetos.

Tal indicação encontra lastro em duas das hipóteses de enquadramento no SRP previstas no art. 3º do Decreto nº 7.892/2013:

- É conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;
- Pela natureza do objeto, não é possível definir previamente o quantitativo a ser demandado pela Administração.

17. ANÁLISE DE RISCOS:

RISCO 1

Descrição do risco:	Elevação do custo da solução em função do preço ser em moeda estrangeira (dólar)
Tipo:	Risco do processo de contratação; Risco de execução do contrato
Probabilidade:	Média
Dano Potencial:	Orçamento insuficiente para viabilizar a contratação
Ação Preventiva:	Optar por um modelo de aquisição que permita a aquisição gradual
Ação Corretiva:	Reduzir o quantitativo adquirido em cada fase da contratação;

RISCO 2

Descrição do risco:	Diminuição do custo da solução em função do preço ser em moeda estrangeira (dólar)
Tipo:	Risco do processo de contratação; Risco de orçamento
Probabilidade:	Média
Dano Potencial:	Sobra de orçamento ao formalizar a contratação
Ação Preventiva:	Não há;
Ação Corretiva:	Informar prontamente à Administração do TSE sobre a aquisição em valor inferior ao estimado

RISCO 3

Descrição do risco:	Insuficiência de capacidade computacional para suportar a solução adquirida
Tipo:	Risco de execução do contrato
Probabilidade:	Baixa
Dano Potencial:	Deficiência no serviço disponibilizado pela ferramenta. Dificuldades para uso e suporte às equipes de desenvolvimento
Ação Preventiva:	Consultar a Coordenadoria de Infraestrutura quanto à disponibilidade da capacidade computacional requerida

RISCO 4

Descrição do risco:	Atraso no recebimento do objeto
Tipo:	Risco de execução do contrato
Probabilidade:	Baixa
Dano Potencial:	Impacto nos projetos que dependem da contratação (incluindo os testes prévios nos produtos que fazem parte do escopo o Teste Público de Segurança a ser realizado em 2019)
Ação Preventiva:	Estabelecer sanções contratuais que inibam o atraso na entrega por parte da eventual contratada; Realizar reunião com a eventual contratada tão logo seja firmado o contrato, para leitura conjunta do contrato e alinhamento de expectativas.
Ação de Contingência:	Continuar utilizando a solução SonarQube+FindSecBugs para as análises estáticas de código
Ação Corretiva:	Aplicar as sanções contratuais previstas

RISCO 5

Descrição do risco:	Modificação da rotina de trabalho das equipes de desenvolvimento
Tipo:	Risco de execução do contrato
Probabilidade:	Média
Dano Potencial:	Subutilização da solução pelas equipes
Ação Preventiva:	Equalizar previamente com as equipes de desenvolvimento a contratação da ferramenta e as consequentes modificações em suas rotinas de trabalho; Prever ações de treinamento para as equipes de desenvolvimento.
Ação Corretiva:	Seprop e equipe de segurança atuarem junto às equipes de desenvolvimento para esclarecer quaisquer problemas que tenham surgido.

RISCO 6

Descrição do risco:	Indisponibilidade orçamentária para manutenção da solução (assinatura e suporte)
Tipo:	Risco operacional
Probabilidade:	Alta
Dano Potencial:	Descontinuidade da solução adquirida após o primeiro ano de uso
Ação Preventiva:	Priorizar alocação de recurso para manutenção da solução (assinatura e suporte)
Ação Corretiva:	Reduzir o número licenças utilizadas

CRONOGRAMA E RESULTADOS DA CONTRATAÇÃO

18. CRONOGRAMAS DE ATIVIDADES PARA ATINGIR O RESULTADO ESPERADO

Item	Atividade	Dada Prevista
1	Elaboração do DOD	Novembro/18
2	Constituição do grupo de contratação	Janeiro e

		Fevereiro/19
3	**Elaboração do Estudo Técnico Preliminar**	**Março/19**
3.1	**Reedição do Estudo Técnico Preliminar, por adequações de forma.**	**Junho/19**
4	**Elaboração do Termo de Referência**	**Março e Abril/19**
5	**Análise do TR pela Seção de Editais**	**Abril a Julho/2019**
6	**Cotação de preço (SAD)**	**Abril a Julho/2019**
7	**Revisão da SCI**	**Abril a Julho/2019**
8	**Elaboração do Edital**	**Abril a Julho/2019**
9	**Revisão pela ASJUR**	**Abril a Julho/2019**
10	**Publicação do Edital**	**Abril a Julho/2019**
11	**Publicação do contrato**	**Abril a Julho/2019**
12	**Início da execução / entrega do objeto**	**Abril a Julho/2019**

19. RESULTADOS PRETENDIDOS

Com a pretendida contratação, busca-se reduzir os problemas associados a falhas de segurança na codificação de sistemas desenvolvidos e/ou mantidos pelo TSE de modo que sejam reduzidas as vulnerabilidades e o impacto dos riscos decorrentes da exploração dessas vulnerabilidades.

Espera-se também que a contratação traga como resultados:

- a redução de diversas falhas de segurança eventualmente decorrentes do desenvolvimento e evolução de sistemas;
- o aumento do ciclo de vida de sistemas;
- a redução de possíveis ataques a falhas de sistemas;
- o aumento da segurança da informação;
- o monitoramento de novas falhas; e
- a redução dos riscos de perda e alteração de informações nos sistemas do TSE.

A lista de benefícios supramencionada não é exaustiva.

20. DECLARAÇÃO DA VIABILIDADE OU NÃO DA CONTRATAÇÃO.

Em virtude da existência de fornecedores capacitados a fornecer o objeto a ser licitado (conforme demonstram as execuções das Provas de Conceito), da inclusão da contratação na Previsão orçamentária e no Planejamento Institucional de 2019, bem como da inexistência de necessidades de adequação do ambiente, a Equipe de Planejamento da Contratação conclui por sua viabilidade.

ANÁLISE E APROVAÇÃO DA AUTORIDADE SUPERIOR

Aprovação da Autoridade Superior

Considerando que foram delimitadas de forma clara e concisa as necessidades da demanda, o alinhamento estratégico, os requisitos da solução, o levantamento das soluções oferecidas pelo mercado e a estratégia e os riscos da contratação, bem como se verifica a pertinência da justificativa da escolha da solução, APROVO o documento em apreço nas estritas disposições apresentadas.

_____, _____ de _____ de 20_____.

_____
(Nome e Matrícula)