TRIBUNAL SUPERIOR ELEITORAL

ANEXO I DO EDITAL - TERMO DE REFERÊNCIA

EDITAL DE LICITAÇÃO TSE Nº 58/2021

MODALIDADE: PREGÃO

FORMA: ELETRÔNICA

SISTEMA DE REGISTRO DE PREÇOS

1. OBJETO

1.1. Registro de preços para eventual aquisição de licença perpétua de uso de *software* para teste e análise estática de segurança de códigos em *softwares* e aplicações (sistemas informatizados), consoante especificações, exigências e prazos constantes deste Termo de Referência.

2. JUSTIFICATIVA

2.1. Os motivos que levaram à presente contratação, as justificativas para solução adotada, as quantidades definidas e demais questões afetas a esse Termo de Referência foram apresentadas no Estudo Preliminar (SEI nº 1085546).

3. ESPECIFICAÇÃO E FORMA DE EXECUÇÃO DO OBJETO

3.1 DESCRIÇÃO DO OBJETO

Lote	Item	Descrição	Unidade de Fornecimento	Quantidade Mínima Estimada	Quantidade
ÚNICO	1	Aquisição de *licença perpétua 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	25	200
	2	Licença perpétua da Console central de gerência	Solução implantada	1	1
	3	Licença perpétua dos Serviços de scanner	Serviço implantado	1	5
	4	Serviço de instalação e configuração da solução	Execução	1	1
	5	Repasse de conhecimento	Execução	1	1
	6	Operação assistida	Execução	1	1

Obs: A quantidade mínima estimada equivalente a 25 projetos foi definida em reunião da CTTI realizada em 22/05/2019, conforme item 9.2.1, à página 3 da respectiva Ata de Reunião (1120697)

3.1.1. A licitante deverá encaminhar proposta de preços especificando marca e modelo do produto ofertado contendo, no mínimo, as informações contidas no modelo de proposta apresentado no Anexo I-V deste Termo.

3.1.2. Caso a solução ofertada não comercialize separadamente os itens 1, 2 e 3, cumprindo-se todos os requisitos deste Termo de Referência, admite-se valor unitário de um centavo de Real (R$ 0,1) para os itens 2 e 3 na proposta prevista no Anexo I-V.

3.2. PRAZO E LOCAL DE ENTREGA

3.2.1. A licença de uso do produto adquirido deverá ser entregue por meio eletrônico ao protocolo do TSE, de segunda a sexta-feira, das 13 às 19 horas.

3.2.2. Os prazos de entrega e execução dos serviços são os seguintes:

3.2.2.1 O prazo conjunto da entrega das licenças de software (Itens 1, 2 e 3) e da realização dos serviços de instalação e configuração (Item 4), será de até 30 (trinta) dias corridos, contados da notificação do contratante, após a publicação do extrato do contrato na Imprensa Oficial.

3.2.2.2 O prazo de início de execução dos serviços de repasse de conhecimento (Item 5) será de até 10 (dez) dias úteis após o término da execução dos serviços de instalação e configuração.

3.2.2.2.1 A data efetiva do início da execução dos serviços de repasse de conhecimento será definida em comum acordo entre o Tribunal e a contratada, observado o prazo máximo definido no item anterior.

3.2.2.2.2 A data efetiva do início da execução dos serviços de repasse de conhecimento poderá ser postergada pelo Tribunal em até 30 (trinta) dias corridos, em função de impossibilidade de participação da equipe no prazo contratual regular.

3.2.2.3 O prazo de início de execução dos serviços de operação assistida (Item 6) será de até 10 (dez) dias úteis após o término da execução do serviço de repasse de conhecimento.

3.2.2.3.1 A data efetiva do início da execução dos serviços de operação assistida será definida pelo Tribunal, respeitado o limite definido no item anterior.

3.2.2.3.2 A data efetiva do início da execução dos serviços de operação assistida poderá ser postergada pelo Tribunal em até 30 (trinta) dias corridos, em função de impossibilidade de início de utilização da solução por parte do Tribunal no prazo contratual regular.

3.2.2.4. Ao Tribunal Superior Eleitoral fica reservado o direito de recusar de pronto o produto que flagrantemente não esteja em conformidade com a descrição do item.

3.3 VALIDADE DAS LICENÇAS

3.3.1. O prazo de validade das licenças deverá ser de, no mínimo, 36 (trinta e seis) meses, contados da data do recebimento definitivo.

3.3.2. As licenças de uso dos softwares (Itens 1, 2 e 3) deverão ser registradas junto ao fabricante em nome do Tribunal Superior Eleitoral, englobando os direitos de atualização de versão e suporte remoto. Tal condição deverá ser comprovada por documento formal emitido pelo fabricante, ou por consulta ao sítio do próprio fabricante na *internet* no prazo previsto no item 3.2.2.1.

4. RECEBIMENTO E PAGAMENTO

4.1. RECEBIMENTO

4.1.1. No momento da entrega das licenças de software (Itens 1, 2 e 3) será emitido o Termo de Recebimento Provisório - TRP, em duas vias, por servidor ou comissão previamente designados, ressalvadas as hipóteses do art. 74 da Lei 8.666/93.

4.1.1.1. O TRP de valor superior a R$ 80.000,00 (oitenta mil reais) deverá ser confiado a uma comissão de, no mínimo, três membros.

4.1.2. Ao final da fase de Instalação e Configuração (Item 4), a contratada deverá encaminhar à equipe de gestão e fiscalização do contrato documento formal indicando a sua conclusão.

4.1.2.1 A partir da segunda adesão do órgão à Ata de Registro de Preços, caso em que não serão contratados os serviços de instalação e configuração, a contratada deverá encaminhar à equipe de gestão e fiscalização do contrato documento formal indicando que o novo conjunto de licenças adquirido foi adicionado à solução previamente instalada e configurada.

4.1.2.2 O fiscal técnico ou comissão designada terão o prazo de até 10 (dez) dias úteis, após o recebimento do documento formalizando o término da instalação e configuração, para emitir o Termo de Recebimento Definitivo - TRD, em duas vias, e remeter o processo ao fiscal administrativo, para pagamento do Itens 1, 2 e 3 e do Item 4, quando for o caso.

4.1.2.3 O TRD compreenderá a verificação da conformidade do software entregue e instalado por meio das análises e conclusões dos quesitos previstos na Lista de Verificação.

4.1.2.4. A Lista de Verificação, definida no Anexo III deste Termo de Referência, evidenciará as avaliações e conclusões realizadas pela fiscalização sobre a conformidade do objeto.

4.1.2.5 Todas as evidências de descumprimento das obrigações assumidas, no todo ou em parte, pela Contratada, deverão constar do TRD para viabilizar a apuração da importância exata a pagar.

4.1.3 Ao final da fase de Repasse de Conhecimento (Item 5) a contratada deverá encaminhar à equipe de gestão e fiscalização do contrato documento formal indicando sua conclusão, acompanhado da lista de presença dos participantes, bem como do Formulário de Avaliação do Repasse de Conhecimento - Anexo I-VI deste Termo de Referência preenchido por todos os participantes.

4.1.3.1 Caso o índice de respostas afirmativas seja inferior a 80% para quaisquer das perguntas, considerado o conjunto dos Formulários de Avaliação do Repasse de Conhecimento preenchidos, o repasse será considerado insatisfatório, e a contratada terá o prazo de até 20 (vinte) dias úteis para sanar as pendências. Persistindo o problema, o serviço será considerado não prestado, incidindo as penalidades contratuais cabíveis.

4.1.3.2 Caso a avaliação do repasse de conhecimento realizada pelos participantes seja positiva, o fiscal técnico ou comissão designada terão o prazo de até 5 (cinco) dias úteis, após o recebimento do documento formalizando o término do Repasse de Conhecimento, para emitir o Termo de Recebimento Definitivo referente ao Repasse de Conhecimento – TRD-RC, em duas vias, e remeter o processo ao fiscal administrativo, para pagamento do Item 5.

4.1.4 Ao final da fase de Operação Assistida (Item 6), a contratada deverá encaminhar à equipe de gestão e fiscalização do contrato documento formal indicando sua conclusão.

4.1.4.1 Caso qualquer dos itens constantes da "**Lista de Verificação 4** - Para a emissão do Termo de Recebimento Definitivo (TRD) referente ao Item 6" não tenha sido observado, a operação assistida será considerada insatisfatória, e a contratada terá o prazo de até 20 (vinte) dias úteis para sanar as pendências, a contar da notificação. Persistindo o problema, o serviço será considerado não prestado, incidindo as penalidades contratuais cabíveis.

4.1.5 O fiscal técnico ou comissão designada terão o prazo de até 5 (cinco) dias úteis, após o recebimento dos documentos formalizando o término do Repasse de Conhecimento e da Operação Assistida, para emitir os Termos de Recebimento Definitivo, em duas vias, e remeter o processo ao fiscal administrativo, para pagamento dos Itens 5 e 6, respectivamente.

4.1.6 Os lançamentos contábeis serão realizados pelas unidades responsáveis da COMPL durante o prazo do recebimento definitivo.

4.1.7 A fiscalização que será realizada pelo TSE não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração, em conformidade com o art. 70 da Lei nº 8.666/93.

4.1.8. Identificada qualquer irregularidade pela fiscalização durante o recebimento do item, a Contratada deverá substituir ou reparar as características reprovadas e cumprir as obrigações pendentes no prazo de até 10 (dez) dias úteis, contados da notificação da fiscalização.

4.1.8.1. Decorrido o prazo ou sanada a incorreção apontada pela fiscalização será reaberto novo prazo para emissão do TRD.

4.1.8.2. O TSE poderá rescindir a contratação caso o item entregue seja novamente reprovado, situação em que será configurada a inexecução total da obrigação assumida, ensejando a aplicação das sanções previstas em lei e no instrumento contratual. Caso não o faça, repetir-se-á o ciclo definido nos itens 4.1.8 e 4.1.8.1 deste Termo de Referência.

4.1.8.3. A contratada deverá desinstalar a solução reprovada no prazo máximo de 10 (dez) dias úteis. Caso não o faça, o Tribunal poderá realizar a desinstalação por qualquer meio que lhe seja disponível.

4.2. PAGAMENTO

4.2.1. O pagamento será efetuado até o 10º (décimo) dia útil, a partir do atesto da nota fiscal/fatura pelo servidor responsável, com a emissão de ordem bancária para o crédito em conta corrente da contratada, observada a ordem cronológica estabelecida no art. 5º da Lei nº 8.666/93.

4.2.1.1. As licenças de uso da solução adquirida, com validade de 36 meses (itens 1, 2 e 3), assim como os serviços (itens 4, 5 e 6), serão pagos em parcela única, após a emissão do TRD de cada item.

4.2.1.2. O atesto do item contratado se dará pelo fiscal administrativo, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto - NTA, conforme previsto na IN nº 14/2017 - TSE. O fiscal administrativo terá o prazo de até 5 (cinco) dias úteis para emitir a NTA e remeter o processo à CEOFI, contados do recebimento do documento fiscal, acompanhado do respectivo Termo de Recebimento Definitivo e dos demais documentos exigidos para liquidação e pagamento da despesa.

4.2.1.3. A Contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento após o recebimento definitivo.

4.2.1.4. Caso o valor faturado não seja superior a R$ 17.600,00, o pagamento será efetuado até o 5º (quinto) dia útil, a partir da apresentação da fatura, conforme § 3º do art. 5º da Lei nº 8.666/93.

4.2.1.5. Na fase de liquidação e pagamento da despesa, a unidade de execução orçamentária e financeira realizará consulta on-line ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou nos sítios de cada órgão regulador, com fins de verificar a regularidade da contratada perante a Seguridade Social e a Fazenda Federal, o Fundo de Garantia por Tempo de Serviço e a Justiça Trabalhista.

5. OBRIGAÇÕES

5.1. OBRIGAÇÕES DA CONTRATADA

5.1.1. Executar, com observação dos prazos e exigências, todas as obrigações constantes deste Termo de Referência.

5.1.2. Responsabilizar-se pelas despesas decorrentes da execução dos serviços objeto deste Termo de Referência.

5.1.3. Informar, no momento da assinatura do contrato, nome do responsável (preposto), os contatos de telefone, e-mail ou outro meio hábil para comunicação com o TSE, bem como manter os dados atualizados durante toda a fase de execução da contratação.

5.1.3.1. Toda a comunicação referente à execução do objeto será realizada através do e-mail informado pela Contratada no momento da assinatura do contrato.

5.1.3.2. A comunicação será considerada recebida após a confirmação de entrega automática encaminhada pelo Outlook, independentemente de confirmação de recebimento por parte da contratada, ficando sob sua responsabilidade a verificação da conta de e-mail.

5.1.3.3. A comunicação só será realizada de forma diversa quando a legislação exigir ou quando a contratada demonstrar ao fiscal os motivos que justifiquem a utilização de outra forma.

5.1.4. Participar de reunião inicial após a formalização contratual, a ser convocada pelo Contratante.

5.1.5. Acatar as recomendações efetuadas pelo fiscal do contrato.

5.1.6. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de culpa ou dolo na execução do objeto do Termo de Referência.

5.1.7. Fazer com que seus empregados se submetam aos regulamentos de segurança e disciplina durante o período de permanência nas dependências do TSE, não sendo permitido o acesso dos funcionários que estejam utilizando trajes sumários (shorts, chinelos de dedo, camisetas regatas ou sem camisa).

5.1.8. Comunicar ao TSE, por escrito, quando verificar condições inadequadas de execução do objeto ou a iminência de fatos que possam prejudicar a sua execução e prestar os esclarecimentos que forem solicitados pelos fiscais.

5.1.9. Manter o caráter confidencial dos dados e informações obtidos por qualquer meio ou prestados pelo TSE, não os divulgando, copiando, fornecendo ou mencionando a terceiros e nem a quaisquer pessoas ligadas direta ou indiretamente à contratada, durante e após a vigência do contrato.

5.1.9.1. Tal exigência se dará de acordo com o "Termo de Compromisso de Manutenção de Sigilo da Informação" cujo modelo consta do Anexo IV deste Termo de Referência, a ser assinado pelos profissionais da contratada que executarão os serviços definidos neste Termo de Referência.

5.1.10. Manter, durante a execução do contrato, as condições de habilitação exigidas na licitação.

5.1.10.1. Verificadas irregularidades nas condições que ensejaram sua habilitação quanto à regularidade fiscal, a contratada terá o prazo de 30 (trinta) dias corridos, contados da notificação da fiscalização, para regularizar a situação, sob pena de aplicação das penalidades cabíveis, sem prejuízo da rescisão do contrato a critério da Administração.

5.1.11. Responsabilizar-se pelos encargos fiscais e comerciais resultantes da contratação.

5.1.11.1. A inadimplência da contratada com referência aos encargos suportados não transfere a responsabilidade por seu pagamento ao contratante, nem poderá onerar o objeto do contrato.

5.1.11.2. No caso de fornecimento de bens importados, a contratada deverá apresentar a documentação que comprove a sua origem, bem como a quitação dos tributos de importação a eles referentes.

5.1.12. Ceder ao Tribunal os direitos de propriedade intelectual e direitos autorais sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, contemplando a documentação gerada, procedimentos estabelecidos para a utilização da solução e quaisquer outros documentos que tenham sido elaborados.

5.2. OBRIGAÇÕES DO CONTRATANTE

5.2.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela contratada.

5.2.2. Acompanhar, fiscalizar e atestar a execução contratual, bem como indicar as ocorrências verificadas.

5.2.3. Designar servidor ou comissão de servidores para fiscalizar a execução do objeto contratual.

5.2.4. Convocar reunião inicial com a Contratada para apresentação do preposto, entrega dos Termos de Compromisso de Manutenção de Sigilo da Informação e outros documentos relevantes, e esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

5.2.5. Permitir que os funcionários da contratada, desde que devidamente identificados, tenham acesso aos locais de entrega.

5.2.6. Recusar qualquer material entregue em desacordo com as especificações constantes do Termo de Referência ou com defeito.

5.2.7. Efetuar o pagamento à contratada segundo as condições estabelecidas neste Termo de Referência.

6. DISPOSIÇÕES GERAIS

6.1. PRAZO DE VIGÊNCIA DO CONTRATO

6.1.1. O contrato terá vigência a partir de ___/___/_____ e duração de 2 (dois) meses.

6.1.2. Os diferentes serviços relacionados no item 3.1 deste Termo têm as seguintes previsões de duração de execução:

Lote	Item	Serviço	Vigência
Único	1	Aquisição de *licença perpétua de software* para teste e análise estática de segurança de códigos em *softwares* e aplicações (sistemas informatizados)	36 meses*
	2	Console central de gerência	36 meses*
	3	Serviços de scanner	36 meses*
	4	Serviço de instalação e configuração da solução	1 mês
	5	Repasse de conhecimento	5 dias úteis
	6	Operação assistida	10 dias úteis

*Prazo derivado da exigência do fornecimento de serviços de suporte técnico remoto pelo fabricante e atualização de versões pelo prazo de, no mínimo, 36 (trinta e seis) meses, não sendo computado para fins de cálculo da vigência contratual.

6.2. REALIZAÇÃO DE PROVA DE CONCEITO

6.2.1. A licitante classificada em primeiro lugar será convocada, pelo pregoeiro, para realizar Prova de Conceito que demonstre o total atendimento da solução ofertada às características e funcionalidades exigidas no edital e especificadas no presente Termo de Referência.

6.2.1.1. A licitante convocada terá um prazo de 5 (cinco) dias úteis para o início da execução da Prova de Conceito. A data efetiva do início da execução deverá ser agendada junto à Coordenadoria de Gestão de TI (COGTI), situado na SAFS Quadra 7 Lotes 1/2, Brasília/DF, Ed. Anexo, Térreo, Sala AV10, telefone (61) 3030-8823.

6.2.1.2. A execução da Prova de Conceito deve ocorrer preferencialmente de forma remota e acompanhada por meio de videoconferências.

6.2.1.3. Por ocasião do agendamento, a licitante convocada deverá indicar, com antecedência mínima de 2 (dois) dias úteis, a composição de sua Equipe Técnica, que poderá ser composta por até 3 (três) profissionais da própria licitante e/ou do fabricante da solução, todos devidamente identificados por meio de vínculo contratual ou procuração.

6.2.1.4. Não será permitida a substituição de qualquer dos componentes da Equipe Técnica da licitante convocada sem a autorização prévia do Tribunal.

6.2.1.5. A data agendada para a realização da Prova de Conceito será divulgada pelo pregoeiro para as demais licitantes.

6.2.1.6. Cada uma das demais licitantes que tenha interesse em acompanhar a Prova de Conceito deverá indicar, com antecedência mínima de 2 (dois) dias úteis, por meio de e-mail ou ofício dirigidos ao pregoeiro, até 2 (dois) profissionais, devidamente identificados por meio de vínculo contratual ou procuração, como "Observadores da Licitante Participante".

6.2.1.7. Não será permitida a substituição de qualquer "Observador da Licitante Participante" sem a autorização prévia do Tribunal.

6.2.1.8. Não será permitida, em hipótese alguma, a comunicação direta entre qualquer "Observador da Licitante Participante" e da "Equipe Técnica da Licitante Convocada", devendo qualquer comunicação ou questionamento ser dirigido unicamente, por escrito, à equipe técnica do Tribunal.

6.2.1.9. A não observância dessa regra de comunicação poderá causar o descredenciamento unilateral e a respectiva retirada do ambiente, por parte do Tribunal, de qualquer dos componentes da "Equipe Técnica da Licitante Convocada" ou de qualquer "Observador da Licitante Participante".

6.2.2 A licitante convocada terá um prazo de 5 (cinco) dias úteis para a realização da Prova de Conceito, a contar da data agendada para seu início, incluindo as ações de instalação da solução e da efetiva realização da avaliação.

6.2.2.1. A COGTI/STI do TSE será responsável pela condução da Prova de Conceito.

6.2.2.2. A licitante deverá instalar sua solução sobre a infraestrutura de virtualização do Tribunal.

6.2.2.2.1. As operações que envolverem acessos físicos ou lógicos a ambientes computacionais do TSE restritos no contexto da segurança cibernética serão executadas pela equipe técnica do TSE com o objetivo de resguardar os ativos envolvidos sendo, portanto, vedado o acesso a tais ambientes por parte das licitantes.

6.2.2.2.2. Cabe à licitante convocada informar, por escrito, a sequência de operações a serem executadas pela equipe técnica do TSE no tocante ao disposto no item 6.2.2.2.1, bem como eventual necessidade de liberação de portas de comunicação entre os ativos envolvidos durante a prova de conceito, sejam eles internos ou externos à rede do TSE.

6.2.2.3. A Prova de Conceito irá aferir a adequação da solução ofertada às necessidades do Tribunal, de acordo com os Critérios de Aceitação da Prova de Conceito (Anexo I-II deste Termo).

6.2.2.4. O não atendimento a qualquer dos Critérios de Aceitação da Prova de Conceito ensejará a desclassificação da licitante convocada do certame.

6.2.2.5. A equipe técnica do Tribunal analisará as eventuais considerações dos observadores das licitantes participantes e fará, caso as julgue pertinentes, solicitação de ajustes de modo a garantir que os testes sejam feitos em conformidade ao estabelecido neste documento.

6.2.2.6. No caso de não ser realizada a Prova de Conceito por motivo imputável à licitante, a proposta será desclassificada, sendo convocadas as licitantes remanescentes, obedecida a ordem de classificação.

6.2.2.7. A licitante participante da Prova de Conceito terá o prazo de 2 (dois) dias úteis, contados a partir do término de sua realização, para desinstalar sua solução.

6.2.2.8. A não desinstalação da solução por parte da licitante ensejará ao Tribunal o direito de realizar a desinstalação por meio de qualquer método que lhe seja disponível.

6.3. SUBCONTRATAÇÃO

6.3.1. É vedado à contratada transferir a outrem, no todo ou em parte, o objeto deste Termo de Referência.

6.4. CRITÉRIOS DE SUSTENTABILIDADE

6.4.1. A solução de software objeto da subscrição 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.

6.4.2. Como condição de participação e durante toda a vigência contratual, sob pena de rescisão, a licitante 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 licitante 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;

6.4.2.1. 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 pelo Ministério do Trabalho e Previdência, 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 e da Justiça Comum, para a licitante e para seus dirigentes.

7. PREÇOS ESTIMADOS

Lote	Item	Descrição	Unidade de Fornecimento	Quantidade	Valores unitários R$	Valores totais R$
ÚNICO	1	Aquisição de *licença perpétua 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	8.031,95	1.606.390,00
	2	Licença perpétua da Console central de gerência	Solução implantada	1	276.836,43	276.836,43
	3	Licença perpétua dos Serviços de scanner	Serviço implantado	5	50.400,73	252.003,65
	4	Serviço de instalação e configuração da solução	Execução	1	236.054,56	236.054,56
	5	Repasse de conhecimento	Execução	1	11.656,79	11.656,79
	6	Operação assistida	Execução	1	21.719,20	21.719,20

ANEXO I-I
ESPECIFICAÇÕES TÉCNICAS

1. Licença perpétua de *software* para teste e análise estática de segurança de códigos em *softwares* e aplicações (sistemas informatizados)

a) Quanto às licenças de uso da solução

1. As licenças da solução de software que equivalem aos Itens 1, 2 e 3 devem ser acompanhadas pelos serviços de suporte técnico remoto pelo fabricante e atualização de versões pelo prazo de, no mínimo, 36 meses.

2. A solução de software equivalente aos Itens 1, 2 e 3 não devem ter tido sua descontinuidade prevista ou publicada pelo fabricante até o momento da abertura da licitação.

b) Quanto à arquitetura da solução

1. Pode ser monolítica ou composta por módulos de sistema de software, desde que sejam do mesmo fabricante, e que se integrem em uma única console de gerenciamento que agregue as funções de administração das configurações da solução e de apresentação das análises de código.
2. A console de gerenciamento deve ser acessível via interface Web.
3. Deve possuir base de dados de vulnerabilidades interna, que deve contemplar ao menos os três conjuntos de vulnerabilidades publicamente disponibilizados abaixo especificados:
    1. Common Weakness Enumeration (CWE);
    2. Common Vulnerabilities and Exposures (CVE);
    3. OWASP Top 10.
4. Deve oferecer atualização da base de dados de vulnerabilidade com frequência mínima trimestral.
5. O servidor ou módulo principal (responsável pela gerência da solução) será instalada sobre a infraestrutura de virtualização existente no TSE, implementada sobre o produto VMware 6.0 (ou superior, caso já tenha sido implantada pelo Tribunal).
6. O padrão do *appliance* virtual utilizado pela solução deverá ser o OVA (*Open Virtual Appliance*).
7. O servidor ou módulo principal deve ser instalado sobre um dos sistemas operacionais abaixo relacionados (cujas licenças de uso serão providas pelo Tribunal):
    1. RedHat Enterprise Linux 7 ou superior;
    2. Microsoft Windows Server 2012 R2 ou superior;
8. O servidor ou módulo principal deve ser instalado sobre um dos Sistemas Gerenciadores de Banco de Dados (SGBDs) abaixo relacionados (no caso da utilização do SGBD Microsoft SQL Server Enterprise, a licença de uso, incluindo os direitos de atualização de versões e suporte técnico remoto, serão providas pela contratada):
    1. PostgreSQL 10.6.1 (ou superior, caso a versão já tenha sido atualizada pelo TSE)
    2. Oracle Database 18C (ou superior, caso a versão já tenha sido atualizada pelo TSE);
    3. Microsoft SQL Server Enterprise;
9. Deve incluir as licenças de uso, incluindo os direitos de atualização de versões e suporte técnico remoto prestado pelo fabricante, de todos os demais softwares comerciais necessários à sua instalação e pleno funcionamento.
10. Deve permitir a autenticação de seus usuários a partir do Microsoft Active Directory.

11. Deve permitir a configuração de perfis de usuários com permissões específicas, para administração da ferramenta, gerenciamento de aplicações cadastradas para avaliação pela ferramenta, submissão de códigos fonte para avaliação pela ferramenta e o respectivo acompanhamento da avaliação, e consulta.
12. Deve possuir mecanismos de auditoria que permitam identificar eventos que envolvam: autenticação de usuários, gerenciamento de usuários, de regras de varredura e das varreduras realizadas.
13. Deve ser fornecida com todos os recursos necessários para integração com as ferramentas abaixo relacionadas:
    1. Jenkins versão 2 e superior: deve permitir a comunicação bidirecional e construção de pontos de barreira (threshold) no processo de construção (build);
    2. GitLab versão 11 e superior: deve ser capaz de obter o código fonte para análise a partir do GitLab; deve prover serviço web que permitam a execução automática de varreduras por meio do acionamento de webhooks do GitLab ou por intermédio do Jenkins;
    3. Subversion (SVN): deve ser capaz de obter o código fonte para análise a partir do SVN;
    4. IDEs Eclipse: deve identificar, interativamente, as vulnerabilidades presentes no código sendo desenvolvido, indicando o trecho afetado e as formas de correção, dentro da própria IDE;
    5. SonarQube versão 7 e superior: Exportar os resultados de análise de vulnerabilidade para o SonarQube;
    6. Softwares de gerenciamento de tickets: possibilitar o acionamento de webservices via tecnologia REST para abertura e atualização de tickets em ferramentas de acompanhamento de casos.
    7. Web APIs: Deve disponibilizar APIs REST que possibilitem no mínimo a visualização das regras de análise e dos resultados de varredura.
14. Deve permitir a adição de pacote de expansão de uso da solução, seja com base em quantidade de usuários, de projetos, de linhas de código, ou de módulos adicionais, de acordo com o modelo de negócios do fabricante ou da arquitetura da solução.
15. Durante o teste de bancada será vedado a configuração ou aplicação de *patches* de qualquer natureza após à disponibilização da solução para o teste.
16. A solução deve ser capaz de realizar mais de uma análise estática em paralelo, sendo que o resultado obtido deve ser o mesmo de análises executadas sequencialmente.

c) Quanto às funcionalidades técnicas

1. Deve ser fornecida com capacidade de analisar o código fonte de aplicações em busca de vulnerabilidades de segurança para, no mínimo, as seguintes linguagens de programação, linguagens de marcação e frameworks:
    1. Java 9 com retrocompatibilidade até Java 6;
    2. JSP, JSF, Angular;
    3. Javascript, Typescript, Ajax;
    4. PHP versões: 5, 7 e superiores;
    5. XML;
    6. HTML;
    7. PL/SQL
    8. C e C++;
    9. Python;
    10. Mobile (Android e IOS);
2. Deve implementar ao menos as seguintes técnicas de análise:
    1. Buffer: detectar vulnerabilidades de "buffer overflow", que envolvam a leitura ou escrita do que o buffer pode gerenciar;
    2. Configuração: detectar problemas de segurança em arquivos de configuração das aplicações;
    3. Conteúdo: detectar problemas de segurança em conteúdo HTML estático e dinâmico, incluindo PHP e JSP;
    4. Estrutural: detectar falhas na estrutura ou definição do programa;
    5. Fluxo de Controle: detectar sequências de operações potencialmente vulneráveis;
    6. Fluxo de Dados: detectar potenciais vulnerabilidades referentes à entrada de dados e à posterior utilização desses dados em operações que ofereçam risco;
    7. Semântica: detectar utilização de funções e APIs de forma potencialmente vulnerável;
3. Deve ser possível a análise de vulnerabilidades sobre códigos fonte completos, trechos de código fonte e arquivos de configuração.
4. As análises de vulnerabilidades devem poder ser realizadas por submissão direta na plataforma, por meio do ambiente de desenvolvimento integrado (IDE) interativamente e por meio da solução de integração contínua especificados neste Termo de Referência.
5. Deve possuir uma interface de linha de comando (CLI), que permita a submissão de análises em projetos analisados previamente ou não na ferramenta.
6. Deve permitir a visualização em tempo real do status das varreduras em execução.
7. Deve permitir ao usuário criar políticas de regras personalizadas que especifiquem quais testes incluir em uma varredura. Tais personalizações deverão ser armazenadas como modelos de configuração de varreduras reutilizáveis, que incluam todos os parâmetros necessários para a execução.

8. Deve permitir a identificação de vulnerabilidades em códigos mal concebidos, ou seja, erros que exponham o sistema a riscos de ataques baseados em fatos identificáveis, tais como, por senhas armazenadas de forma não apropriada.
9. Deve permitir a indicação de falso-positivos (detecção errônea de vulnerabilidades) e a inclusão de comentários referentes às vulnerabilidades encontradas, mantendo-se o histórico nas análises subsequentes. Em ambos os casos, deve armazenar a identificação do usuário, data e hora do registro.
10. Deve possuir capacidade para produzir alertas para cada tipo de vulnerabilidade única que for identificada. Tais alertas devem conter as seguintes informações:
    1. Trecho do código vulnerável;
    2. Descrição da vulnerabilidade;
    3. Código de referência de bases de vulnerabilidades conhecidas, tais como CVE, VulnDB, CWE, NVD, se houver;
    4. Nível de severidade;
    5. Guia de remediação;
    6. Exemplos de código de remediação;
11. Deve permitir a organização das vulnerabilidades identificadas em grupos para facilitar o processo de triagem e correção.
12. Deve possibilitar ao usuário a definição de filtros para os resultados de uma varredura, permitindo focar em determinados tipos de apontamento, tais como: tipo de vulnerabilidade, base de vulnerabilidade, risco potencial, API, arquivo ou diretório onde se encontra o código fonte vulnerável.
13. Deve permitir ao usuário desabilitar regras de análise, alterar o seu nível de severidade e identificar quais regras de detecção de vulnerabilidades foram desabilitadas.
14. Deve permitir que o usuário crie regras de detecção, identificando uma vulnerabilidade que a ferramenta não foi capaz de detectar nativamente.
15. Deve exibir de forma gráfica as informações para a identificação da vulnerabilidade, incluindo o ponto de entrada na aplicação, as saídas, bem como quaisquer outros pontos intermediários.
16. Deve permitir a determinação de ponto de barreira (threshold), ou seja, conjunto de precondições estabelecidas pelo administrador da ferramenta, a ser considerado no processo de construção (build) da aplicação, como condição de sucesso ou falha.
17. Deve possuir capacidade de análise incremental, que realiza análise somente em conjunto de código modificado a partir de uma "baseline" determinada, possibilitando a redução do tempo total de análise.
18. Deve permitir a comparação entre duas varreduras executadas sobre o mesmo código-fonte, apresentando as diferenças através de relatório.
19. Deve gerar relatórios sobre as vulnerabilidades encontradas de pelo menos duas formas: relatório gerencial e relatório detalhado com todas as informações técnicas necessárias.
20. Deve oferecer a possibilidade de geração de relatórios em conformidade com o OWASP Top 10 em sua versão mais atual.
21. Deve incluir no relatório o trecho do código fonte onde foi encontrada a vulnerabilidade.
22. Deve apresentar o resultado da análise em Português ou Inglês.
23. Deve gerar relatórios em formatos distintos, incluindo ao menos os formatos:
    1. Para leitura por usuários: PDF ou HTML
    2. Para processamento por outros softwares, XML, JSON ou CSV.
24. Deve possuir Dashboards das análises realizadas que possibilitem ao administrador configurar, dentre as informações gerenciadas pela ferramenta, aquelas que deseja apresentar em sua interface.

d) Quanto aos serviços do fabricante associados às licenças de software

1. Direito de atualização de versões da solução, incluindo todos os seus componentes licenciados, durante o período de validade das licenças;
2. Suporte técnico remoto, em português, acionável por interface web ou por telefone no Brasil, para o esclarecimento de dúvidas quanto à utilização da solução, ou para a submissão de problemas de funcionamento da solução;
    1. O suporte técnico será acionado por meio da abertura de chamados técnicos, que conterá, além do detalhamento da solicitação de suporte, a indicação de seu nível de severidade;
    2. O serviço de suporte técnico deverá suportar a definição de ao menos três níveis de severidade, cujas características e tempos de resolução (definitiva ou de contorno) são os especificados na tabela abaixo

Severidade	Descrição	Tempo de Atendimento
Alta	Solução sem condições de utilização	Até 2 dias úteis
Média	Solução em operação, porém com funcionalidades importantes sem condições de utilização	Até 6 dias úteis
Baixa	Todos os demais problemas ou solicitações de orientação de uso	Até 15 dias úteis

3. Em caso de a solução apresentada não ser definitiva (solução de contorno), o fornecedor deverá apresentar ao TSE plano de solução definitiva em até 10 dias úteis.
4. Acesso à base de conhecimento do fabricante, tanto referente ao funcionamento da solução quanto referente às vulnerabilidades de código por ela reconhecidas.

2. Serviço de instalação e configuração da solução

1. Instalar a solução e todos os componentes dos quais a mesma dependa para seu funcionamento, como, por exemplo, sistema operacional, banco de dados, servidor de aplicação e outros.
    1. A instalação dos componentes deverá observar os padrões de configuração e de segurança estabelecidos pelo Tribunal, no que não conflitar com os requisitos da solução. Eventuais conflitos devem ser documentados, incluindo as soluções de contorno aplicáveis para mitigar eventuais riscos.
2. Incluir e configurar ao menos um usuário pertencente a cada perfil de acesso definido pelo Tribunal.
3. Configurar as integrações com ao menos uma instância dos ambientes de IDE, Versionador de códigos, Integração contínua e Qualidade de software.
4. Fornecer ao Tribunal, em conjunto com a entrega do documento indicativo de finalização do serviço de instalação e configuração, citado no item 4.1.2 do Capítulo 4 do Termo de Referência, a documentação referente a cada uma das atividades acima descritas, de forma a possibilitar a execução de tais configurações pela equipe interna.
5. Opcionalmente, o serviço poderá ser realizado por meio de recursos de video-conferência e acesso remoto, por comum acordo entre o Contratante e a Contratada.

3. Repasse de conhecimento

1. Ministrar repasse de conhecimento sobre a solução, dividido em turmas distintas conforme o escopo, na forma indicada a seguir:
    1. 1 (uma) turma para 6 (seis) profissionais, contemplando os administradores da solução os administradores de infraestrutura, a respeito da administração da solução, bem como das peculiaridades de instalação e configuração no ambiente do Tribunal;
    2. 2 (duas) turmas para 12 (doze) profissionais cada uma, contemplando os servidores do Tribunal envolvidos com aspectos de desenvolvimento de software.
2. A carga horária mínima total para cada turma deverá ser de 20 horas, observado o limite máximo de 4 horas diárias, compreendidas no período de 14h às 19h, em dias úteis.
    1. O efetivo horário de realização do repasse para cada turma poderá ser ajustado em comum acordo pelo Tribunal e pela contratada, observando-se os limites acima indicados.
3. Deverá ser ministrado nas dependências do Tribunal, que se responsabilizará pela disponibilização de ambiente dotado de estações de trabalho e projetor.
    1. Opcionalmente poderá ser realizado por meio de recursos de video-conferência e acesso remoto, por comum acordo entre o Contratante e a Contratada.
4. Os demais recursos referentes ao repasse de conhecimento serão de responsabilidade da contratada, incluindo, mas não se limitando a,recursos humanos, licenças e instalação dos softwares necessários.
5. Deverá ser ministrado por profissional certificado ou acreditado pelo FABRICANTE, e deverá ser baseado em documentação técnica oficial da solução de análise de vulnerabilidades, podendo conter os devidos ajustes, desde que homologados pela representante da FABRICANTE no BRASIL e aceitos pelo Tribunal.
6. Deverá ser fornecido todo material didático, em Português do Brasil, necessário ao pleno acompanhamento, por parte dos instruendos, dos assuntos a serem ministrados durante o referido repasse de conhecimento;
7. Deverá contemplar, no mínimo, os seguintes tópicos:
    1. Características de instalação e configuração da solução no ambiente computacional do TSE;
    2. Administração da solução;
    3. Conexão com o Jenkins (ambiente de integração contínua);
    4. Conexão com o GitLab e SVN (sistemas de controle de versão);
    5. Integração com a IDE Eclipse;
    6. Integração com o SonarQube;
    7. Inclusão e exclusão de projetos de software na solução;
    8. Realização de análises de vulnerabilidades a partir da interface da própria ferramenta, bem como envolvendo as integrações com as ferramentas Jenkins, GitLab, SVN, IDE Eclipse e SonarQube;
    9. Correção das vulnerabilidades apontadas pela solução;
    10. Realização de ciclo completo de verificação de erros/vulnerabilidades, para verificar o reflexo das correções inseridas no código e os respectivos relatórios gerados;
    11. Identificação, classificação e gerenciamento das partes dos códigos-fontes apontados como pontos de vulnerabilidades;
    12. Criação de novas regras e gerência das regras existentes;
    13. Geração de relatórios;
    14. Configuração de dashboards;
    15. O repasse de conhecimento deverá contemplar a apresentação teórica das funcionalidades da solução e atividades práticas.

4. Operação assistida

1. Prestar operação assistida nas dependências do Tribunal durante 10 (dez) dias úteis após a emissão do Termo de Recebimento Definitivo - TRD.
2. A operação assistida consistirá na presença nas dependências do Tribunal de um profissional certificado ou acreditado pelo fabricante da solução fornecida, durante o período das 14h às 19h.
    1. Opcionalmente poderá ser realizada por meio de recursos de video-conferência e acesso remoto, por comum acordo entre o Contratante e a Contratada.
3. Este profissional será responsável por atender prontamente a qualquer solicitação de esclarecimentos por parte da equipe de administração da solução no Tribunal, ou por parte das equipes de desenvolvimento que estiverem utilizando o produto, bem como a qualquer ocorrência de problema no funcionamento da solução, incluindo suas integrações que tenham sido configuradas com os demais ambientes de desenvolvimento de *software* do Tribunal.

ANEXO I-II

CRITÉRIOS DE ACEITAÇÃO DA PROVA DE CONCEITO

QUANTO À ARQUITETURA DA SOLUÇÃO		
Item	**Descrição**	**Critério de Aceitação**
a.i	Pode ser monolítica ou composta por módulos de sistema de software, desde que sejam do mesmo fabricante, e que se integrem em uma única console de gerenciamento.	- Documentação disponível no site ou documento c fabricante comprovando a origem comum de todos os m - Acesso por meio da console de gerenciamento a módulos da solução ofertada.
a.ii	A console de gerenciamento deve ser acessível via interface Web.	- Acesso, via navegador Web, ao módulo cer gerenciamento.
a.iii	Deve possuir base de dados de vulnerabilidades interna, que deve contemplar ao menos os três conjuntos de vulnerabilidades publicamente disponibilizados abaixo especificados.	- Acesso às bases de vulnerabilidades da solução por console de gerenciamento, e verificação de sua conf com as bases publicadas especificadas no Termo de Refe
a.iv	Deve oferecer atualização da base de dados de vulnerabilidade com frequência mínima trimestral.	- Documentação disponível no site ou documento c fabricante comprovando política de atualização de r vulnerabilidade implementada sobre a solução;
a.v	O servidor ou módulo principal (responsável pela gerência da solução) será instalado sobre a infraestrutura de virtualização existente no TSE, implementada sobre o produto VMware 6.0 (ou versão superior, caso já tenha sido implantada pelo Tribunal)	- Solução instalada em servidor virtualizado, verificável do vCenter;
a.vi	O padrão do *appliance* virtual utilizado pela solução deverá ser o OVA (*Open Virtual Appliance*).	O formato do *appliance* virtual deve ser o OVA (*Ope Appliance*).
a.vii	O servidor ou módulo principal deve ser instalado sobre um dos sistemas operacionais abaixo relacionados (cujas licenças de uso serão providas pelo Tribunal)	- Servidor ou módulo principal efetivamente instalad infraestrutura de virtualização do Tribunal, e verific processos ou serviços sendo executados sobre o servid solução tenha sido instalada.
a.viii	O servidor ou módulo principal deve ser instalado sobre um dos Sistemas Gerenciadores de Banco de Dados (SGBDs) abaixo relacionados (no caso da utilização de SGBD comercial, as licenças de uso, incluindo os direitos de atualização de versões e suporte técnico remoto, serão providas pela contratada)	- Banco de dados implantado e acessível via co gerenciamento própria, sobre o SGBD indicado na comercial da contratada.
a.ix	Deve incluir as licenças de uso, incluindo os direitos de atualização de versões e suporte técnico remoto, de todos os demais softwares comerciais necessários à sua instalação e pleno funcionamento	- Não verificável em tempo de Prova de Conceito.
a.x	Deve permitir a autenticação de seus usuários a partir do Microsoft Active Directory	- Usuário existente no AD do TSE e autenticado na ofertada.
a.xi	Deve permitir a definição de perfis de usuários com permissões específicas, para administração da ferramenta, gerenciamento de aplicações cadastradas para avaliação pela ferramenta, submissão de códigos fonte para avaliação pela ferramenta e o respectivo acompanhamento da avaliação, e consulta.	- Os diferentes perfis devem ser criados, diferentes devem ser associados a esses perfis, e seus direitos c devem ser verificados conforme funcionalidades habilit respectivos perfis.
a.xii	Deve possuir mecanismos de auditoria que permitam identificar eventos que envolvam: autenticação de usuários, gerenciamento de usuários, de regras de varredura e das varreduras realizadas.	- As operações definidas neste item devem ser realizada ferramenta, e os respectivos registros de atividad acessíveis e consultáveis.

a.xiii	Deve ser fornecida com todos os recursos necessários para integração com as ferramentas abaixo relacionadas.	- Jenkins: - Apresentar documentação demonstrando o suporte à v Jenkins especificada neste Termo de Referência. - Demonstrar o Jenkins disparando uma varre vulnerabilidade e recebendo o resultado da análise. - Gitlab: - Apresentar documentação demonstrando o suporte à v Gitlab especificada neste Termo de Referência. - Verificar a capacidade de a ferramenta obter um cód armazenado no Gitlab e utilizá-lo em uma varredura. - Verificar a capacidade de a ferramenta ser acionada de um webhook configurado no Gitlab. - SVN: - Apresentar documentação demonstrando o suporte à v SVN especificada neste Termo de Referência. - Verificar a capacidade de a ferramenta obter um cód armazenado no SVN e utilizá-lo em uma varredura. - IDE: - Apresentar documentação demonstrando integraçã IDEs Eclipse. - Demonstrar interativamente a análise de segurança d que está sendo implementado. - SonarQube: - Apresentar documentação demonstrando o suporte à v SonarQube especificada neste Termo de Referência. - Acessar os resultados da análise de uma varredura ex para o SonarQube. - Ferramenta de Gerenciamento de Tickets: - Apresentar documentação que comprove a possibil acionamento de um webservice remoto via REST para a atualização de um ticket. - Web APIs: - Apresentar documentação da Web API fornec ferramenta, comprovando a possibilidade de visualiz regras de uma análise por meio de uma chamada a We obtenção do resultado de uma análise.
a.xiv	Deve permitir a adição de pacote de expansão de uso da solução, seja com base em quantidade de usuários, de projetos, de linhas de código, ou de módulos adicionais, de acordo com o modelo de negócios do fabricante ou da arquitetura da solução.	- Documentação disponível no site ou documento d fabricante comprovando as formas de expansão;
a.xv	Durante o teste de bancada será vedado a configuração ou aplicação de *patches* de qualquer natureza após à disponibilização da solução para o teste.	- Não ter configurações ou patches instalados disponibilização para o teste de bancada.
a.xvi	A solução deve ser capaz de realizar mais de uma análise estática em paralelo, sendo que os resultados obtidos devem ser os mesmos de análises executadas sequencialmente.	- Os resultados obtidos de execuções de análises em devem ser os mesmos das análises executadas sequenci
QUANTO ÀS FUNCIONALIDADES TÉCNICAS		
b.i	Deve ser fornecida com capacidade de analisar o código fonte de aplicações em busca de vulnerabilidades de segurança para, no mínimo, as seguintes linguagens.	- Documentação disponível no site ou documento d fabricante comprovando as linguagens suportadas; - Será feita a verificação da execução de análise de ao (três) linguagens, a critério do TSE.
b.ii	Deve utilizar técnicas de análise que incluam, no mínimo, a análise de fluxo de controle (sequência de operações), análise de buffer, fluxo de dados, análise semântica e estrutural.	- Documentação disponível no site ou documento d fabricante comprovando as técnicas de análise utiliza solução.
b.iii	Deve ser possível a análise de vulnerabilidades sobre códigos fonte completos, trechos de código fonte e arquivos de configuração.	- Execução da análise de códigos fonte completos, tr código fonte e arquivos de configuração fornecidos pelo
b.iv	As análises de vulnerabilidades devem poder ser realizadas por submissão direta na plataforma, por meio do ambiente de desenvolvimento integrado (IDE) interativamente e por meio da solução de integração contínua especificados neste Termo de Referência.	- Execução de análises a partir de cada uma das especificadas.
b.v	Deve possuir uma interface de linha de comando (CLI), que permita a submissão de análises em projetos analisados previamente ou não na ferramenta.	- Execução de análise a partir da linha de comand projeto(s) selecionados pelo TSE.
b.vi	Deve permitir a visualização em tempo real do status das varreduras em execução.	- Status das varreduras em execução visualizados em te na console de gerenciamento.
b.vii	Deve permitir ao usuário criar políticas de regras personalizadas que especifiquem quais testes incluir em uma varredura. Tais personalizações deverão ser armazenadas como modelos de configuração de varreduras reutilizáveis, que incluam todos os parâmetros necessários para a execução.	- Política de teste criada, armazenada como modelo, e v efetivamente realizada de acordo com a política definida
b.viii	Deve permitir a identificação de vulnerabilidades em códigos mal concebidos, ou seja, erros que exponham o sistema a riscos de ataques baseados em fatos identificáveis, tais como, por senhas armazenadas de forma não apropriada.	- Execução de análise sobre código fornecido pelo contenha senha armazenada de forma não apropriada.

b.ix	Deve permitir a indicação de falso-positivos (detecção errônea de vulnerabilidades) e a inclusão de comentários referentes às vulnerabilidades encontradas, mantendo-se o histórico nas análises subsequentes. Em ambos os casos, deve armazenar a identificação do usuário, data e hora do registro.	- Indicação de falso positivo e de comentário sobre um efetivamente realizada durante a POC. Verificação do re identificação do usuário, data e hora do registro, be persistência dessas indicações sobre análises futuras.
b.x	Deve possuir capacidade para produzir alertas para cada tipo de vulnerabilidade única que for identificada. Tais alertas devem conter as seguintes informações:	- Alertas emitidos pela solução, em análise efet executada na POC, devem incluir as informações rela neste Termo de Referência.
b.xi	Deve permitir a organização das vulnerabilidades identificadas em grupos para facilitar o processo de triagem e correção.	- Vulnerabilidades efetivamente alertadas pela solução, POC, devem ser agrupadas e, a partir do agrupamento, possível a tomada de ações de triagem e correção.
b.xii	Deve possibilitar ao usuário a definição de filtros para os resultados de uma varredura, permitindo focar em determinados tipos de apontamento, tais como: tipo de vulnerabilidade, base de vulnerabilidade, risco potencial, API, arquivo ou diretório onde se encontra o código fonte vulnerável.	- Construção dos filtros definidos no Termo de Refe verificação de seu correto funcionamento.
b.xiii	Deve permitir ao usuário desabilitar regras de análise e identificar quais regras de detecção de vulnerabilidades foram desabilitadas.	- Desativação de uma regra na interface e sua identifica regra desativada.
b.xiv	Deve permitir que o usuário crie regras de detecção, identificando uma vulnerabilidade que a ferramenta não foi capaz de detectar nativamente.	- Demonstração do mecanismo de criação de personalizadas.
b.xv	Deve exibir de forma gráfica as informações para a identificação da vulnerabilidade, incluindo o ponto de entrada na aplicação, as saídas, bem como quaisquer outros pontos intermediários.	- Demonstração da forma gráfica para identific vulnerabilidade.
b.xvi	Deve permitir a determinação de ponto de barreira (threshold), ou seja, conjunto de precondições estabelecidas pelo administrador da ferramenta, a ser considerado no processo de construção (build) da aplicação, como condição de sucesso ou falha.	- Demonstrar a condição de falha ou sucesso no pro build em função dos resultados da análise de vulnerabi código fonte.
b.xvii	Deve possuir capacidade de análise incremental, que realiza análise somente em conjunto de código modificado a partir de uma "baseline" determinada, possibilitando a redução do tempo total de análise.	- Realização efetiva de análise sucessivas sobre o mesm e verificação do caráter incremental.
b.xviii	Deve permitir a comparação entre duas varreduras executadas sobre o mesmo código-fonte, apresentando as diferenças através de relatório	- Apresentar relatório comparativo entre as duas varred
b.xix	Deve gerar relatórios sobre as vulnerabilidades encontradas de pelo menos duas formas: relatório gerencial e relatório detalhado com todas as informações técnicas necessárias.	- Efetiva geração de ambos os relatórios sobre ar vulnerabilidade realizada durante a POC.
b.xx	Deve oferecer a possibilidade de geração de relatórios em conformidade com o OWASP Top 10 em sua versão mais atual.	Efetiva geração de relatório sobre análise de vulner realizada durante a POC, com a visão de acordo com Top 10.
b.xxi	Deve incluir no relatório o trecho do código fonte onde foi encontrada a vulnerabilidade.	Efetiva geração de relatório sobre análise de vulner realizada durante a POC, incluindo o trecho de código re
b.xxii	Deve apresentar o resultado da análise em Português ou Inglês.	Resultados das análises, visualizados tanto pela(s) int da solução como por relatórios por ela gerados, expr Português ou Inglês.
b.xxiii	Deve gerar relatórios em formatos distintos, incluindo ao menos os formatos: 1. Para leitura por usuários: PDF ou HTML 2. Para processamento por outros softwares, XML, JSON ou CSV.	Relatórios com conteúdos idênticos gerados em formatos relacionados no Termo de Referência.
b.xxiv	Deve possuir Dashboards das análises realizadas que possibilitem ao administrador configurar, dentre as informações gerenciadas pela ferramenta, aquelas que deseja apresentar em sua interface	- Visualização da funcionalidade de Dashboards e r capacidade de configuração.

ANEXO I-III
LISTAS DE VERIFICAÇÃO

Lista de Verificação 1 - Para a emissão do Termo de Recebimento Provisório (TRP) referente aos Itens 1, 2 e 3

Item	Situação Observada	Aceitação (Sim/Não)
Verificar se o documento de licenciamento foi emitido corretamente em nome do TSE, e em data posterior à homologação do pregão.		
Conferência do quantitativo de licenças indicadas no documento de licenciamento, conforme a especificação prevista neste Termo e na proposta de preço		
Conferência do aspecto qualitativo (inclusive marca e modelo), conforme a especificação prevista neste Termo e na proposta de preço		
Outras observações consideradas pertinentes pela fiscalização		

Lista de Verificação 2 - Para a emissão do Termo de Recebimento Definitivo (TRD) referente aos Itens 1, 2, 3 e 4

Item	Situação Observada	Aceitação (Sim/Não)
Conferência da instalação realizada quanto ao quantitativo contratado		
Conferência do aspecto qualitativo (inclusive marca e modelo), conforme a especificação prevista neste Termo e na proposta de preço		
Testes de funcionamento da solução instalada, incluindo as integrações com os demais ambientes de desenvolvimento		
Cumprimento das demais obrigações previstas no Termo de Referência, referentes à subscrição de software e sua instalação e configuração		
Outras observações consideradas pertinentes pela fiscalização		

Lista de Verificação 3 - Para a emissão do Termo de Recebimento Definitivo (TRD) referente ao Item 5

Item	Situação Observada	Aceitação (Sim/Não)
Verificar se o documento que formaliza a realização do Repasse de Conhecimento foi corretamente emitido pela Contratada em nome do Tribunal, e se a data está compatível com os prazos aplicáveis.		
Verificar se a Lista de Presença identifica corretamente os participantes, e se foi corretamente preenchida por estes.		
Verificar se o índice de respostas afirmativas quanto a todas as perguntas constantes do formulário de avaliação do Repasse de Conhecimento foi superior a 80%.		

Lista de Verificação 4 - Para a emissão do Termo de Recebimento Definitivo (TRD) referente ao Item 6

Item	Situação Observada	Aceitação (Sim/Não)
Verificar se o documento que formaliza a realização da Operação Assistida foi corretamente emitido pela Contratada em nome do Tribunal, e se a data está compatível com os prazos aplicáveis.		
Verificar se o documento que formaliza a realização da Operação Assistida indica que a mesma foi cumprida por profissional certificado ou acreditado pelo fabricante da solução fornecida.		
Verificar se todos os pedidos de esclarecimentos ou de suporte técnico foram satisfatoriamente atendidos		
Verificar se foi gerado o relatório de recomendações decorrentes do período de operação assistida		

ANEXO I-IV
TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO DA INFORMAÇÃO

A **<Nome da Empresa>**, empresa inscrita no CNPJ sob o nº **XX.XXX.XXX/XXXX-XX** com endereço na **<endereço da empresa>**, neste ato representada por meio de seu representante legal ao fim assinado, doravante designada "**<Nome simplificado da empresa>**", pelo presente Termo, assume o compromisso de manutenção de sigilo sobre as informações a que tenha acesso ou conhecimento no âmbito do Tribunal em razão das atividades profissionais a serem realizadas em decorrência dos serviços de consultoria em segurança da informação a serem prestados ao TSE.

Compromete-se a não divulgá-las ou comentá-las interna ou externamente e cumprir as condutas adequadas contra destruição, modificação, divulgação indevida e acesso indevido, seja acidental ou intencionalmente.

Está ciente de que este Termo se refere a todas as informações do Tribunal – dados, processos, informações, documentos e materiais – seja qual for o meio através do qual sejam apresentadas ou compartilhadas: escritas em papel ou nos sistemas eletrônicos, faladas em conversas formais e informais, disseminadas nos meios de comunicação internos como reuniões, televisão, etc.

Este compromisso permanece mesmo após a conclusão dos serviços ora prestados.

Declara que o Tribunal tem sua permissão prévia para acesso e monitoramento do ambiente de trabalho onde serão desenvolvidos os serviços objeto do presente termo.

Brasília, de de 2021.

_____

<Nome da empresa>

Representante Legal

Nome:_____

CPF: _____

RG: _____

ANEXO I-V - MODELO DE PROPOSTA			
Razão social:		E-mail:	CNPJ:
Endereço:	Cidade:	CEP:	Tel.:

Planilhas de formação de preços:

Lote	Item	Descrição*	Marca/Modelo e demais observações	Unidade de Fornecimento	Quantidade	Valor unitário (R$)	Valor total (R$)
ÚNICO	1						
	2						
	3						
	4						
	5						
	6						
	Valor total do lote (R$)						

* A licitante deve detalhar a especificação do objeto a ser fornecido e/ou prestado.

Declarações:

i) Esta empresa declara que tem pleno conhecimento das condições necessárias para a execução do objeto.

ii) Esta empresa declara que nos preços propostos acima estão incluídas todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto desta Licitação.

iii) Esta empresa declara estar ciente de que a apresentação da presente proposta implica na plena aceitação das condições estabelecidas no Edital e seus Anexos

Validade da Proposta:

O prazo de validade desta proposta é de ___ (<*não inferior a 60 dias*>) dias, contados da data de abertura do Pregão.

Local e data

Nome do Responsável Legal
Cargo/Função

ANEXO I-VI

FORMULÁRIO DE AVALIAÇÃO DO REPASSE DE CONHECIMENTO

Nome completo:

Matrícula:

Lotação:

Assinale com "X" a coluna "SIM" ou "NÃO", de acordo com a sua avaliação.

ITEM DE AVALIAÇÃO	SIM	NÃO
1) O profissional da contratada demonstrou domínio sobre o assunto?		
2) Todos os tópicos obrigatórios de repasse de conhecimento foram realizados (item 7)?		
3) Todas as dúvidas apresentadas pelos servidores foram sanadas?		
4) A documentação correspondente foi disponibilizada?		

Brasília, ____ de _____ de _____

ANEXO I-VII

FORMULÁRIO DE INDICAÇÃO DE PREPOSTO

A empresa **Nome da Empresa**, com sede na **Endereço da empresa**, na cidade de **Cidade**, (**UF**), CNPJ nº **000.000.000/0000-0**, neste ato representada pelo seu **Cargo do Representante**, Senhor(a) **Nome do Representante** portador(a) da Carteira de Identidade nº **Identidade do Representante**, CPF nº **CPF do Representante**, em atenção ao art. 44 da IN MPDG nº 5/2017, DESIGNA, o(a) Senhor(a) **Nome do Colaborador**, portador(a) da Carteira de Identidade nº **Identidade do Colaborado**, CPF nº **CPF do Colaborador**, para atuar como preposto no âmbito do **Contrato TSE nº ___/2021.**

2. O preposto designado representará a empresa perante o Tribunal Superior Eleitoral, zelará pela boa execução do objeto contratual, exercendo os seguintes poderes e deveres:

a)	
b)	
c)	

3. A comunicação entre o preposto e o Tribunal Superior Eleitoral será efetuada por meio do telefone **(DDD)00000-0000** ou do e-mail **email@email.com.br.**

4. A **Nome da Empresa** compromete-se a manter atualizados, durante toda fase de execução da contratação, os contatos de telefone e e-mail para comunicação com o Tribunal Superior Eleitoral.

JOSÉ RODRIGUES DE ARAÚJO NETO
SECRETÁRIO(A) DE ADMINISTRAÇÃO - SUBSTITUTO(A)

Documento assinado eletronicamente em **13/09/2021, às 12:18**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1776694&crc=32B7C597, informando, caso não preenchido, o código verificador **1776694** e o código CRC **32B7C597.**