TRIBUNAL SUPERIOR ELEITORAL

ESTUDOS TÉCNICOS PRELIMINARES

I - Necessidade a ser atendida pela contratação:

Executar, de forma coerente em toda a Justiça Eleitoral, os serviços especializados previstos pela Estratégia Nacional de Cibersegurança.

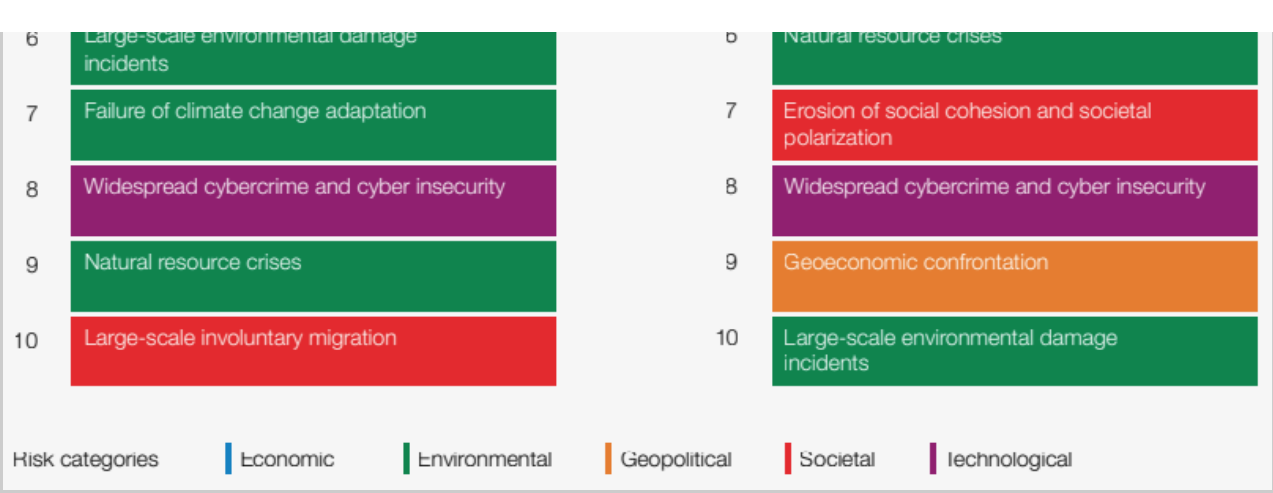
II - Indique a(s) consequência(s), caso não haja atendimento da necessidade:

Conforme registrado no documento da Estratégia Nacional de Cibersegurança (Processo SEI 2021.00.000005110-1, documento nº 1759818):

> *"Um dos eixos estruturantes mais importantes para o ganho acelerado em maturidade que a Justiça Eleitoral precisa ter para fazer frente aos grandes desafios das Eleições 2022 é a contratação de serviços especializados. Por meio dessa contratação, que propomos ser conduzida centralizadamente pelo TSE, com disponibilidade de serviços em todos os Tribunais Regionais,* ***pretende-se atacar questões fundamentais para as quais o corpo técnico hoje presente na Justiça Eleitoral ainda precisa ganhar em habilidade e capacitação****.*
>
> ***Assim, a contratação de serviços faz-se imperiosa pela necessidade de ganho acelerado de capacidades que não estão presentes hoje na J.E****"* (grifos nossos)

Muito embora a Estratégia Nacional de Cibersegurança tenha citado que a contratação de serviços especializados de segurança seria essencial para as Eleições de 2022, a necessidade desses serviços se estende para além desse período, sendo uma questão perene para a Justiça Eleitoral, uma vez que os riscos associados ao ambiente cibernético são constantes, gerando, portanto, uma demanda contínua de ações de proteção, monitoramento e defesa cibernética.

Com efeito, o relatório "Global Risks Report - 2023" publicado pelo World Economic Forum classifica cibercrimes e insegurança cibernética (Widespread cybercrime and cyberinsecurity) como o oitavo risco mais significativo, em escala global, tanto a curto prazo (2 anos - 2 years) quanto a longo prazo (10 anos - 10 years), conforme imagem abaixo:



Fonte: WEF_Global_Risks_Report_2023.pdf (weforum.org)

O próprio World Economic Forum , em seu relatório "Global Security Outlook Report - 2023" [1], especificamente voltado a questões de cibersegurança, nos apresenta o seguinte cenário:

> "**Geopolitical instability**, rapidly maturing and emerging technologies, **lack of available talent**, and increasing **shareholder** and regulatory expectations represent some of the significant challenges that concern **cyber** and business **leaders**."

Em tradução livre:

> "**Instabilidade geopolítica**, tecnologias emergentes e de rápida maturação, **ausência de talentos disponíveis**, e expectativas crescentes tanto de **partes interessadas** quanto regulatórias representam alguns dos desafios significativos que atingem os **líderes cibernéticos** e de negócios." (grifos nossos)

O clima de tensão que circundou o processo eleitoral de 2022 demonstra, de forma cabal, que a segurança desse processo é de vital importância para que a sociedade brasileira, como parte interessada, tenha confiança no resultado das eleições. Por sua vez, a observação do World Economic Forum de que a ausência de talentos disponíveis é um desafio para os líderes cibernéticos coincide com a informação trazida pela Estratégia Nacional de Cibersegurança quanto à "*necessidade de ganho acelerado de capacidades que não estão presentes hoje na J.E.*".

Nesse contexto, a contratação de serviços nacionais de cibersegurança, que disponibilizem à Justiça Eleitoral serviços tais como o Diagnóstico e Análise de maturidade dos Tribunais Eleitorais (necessário para melhor direcionar os esforços em cibersegurança), a realização de Simulações de Ataque, (que têm como objetivo identificar lacunas de conhecimentos e habilidades das equipes internas com relação à defesa contra ataques cibernéticos), análise de vulnerabilidade de aplicações, dentre outros, demonstra-se essencial para que a Justiça Eleitoral possa elevar, de forma conjunta, seu nível de maturidade em cibersegurança.

A não contratação de tais serviços, portanto, causaria dificuldades e atrasos no ganho desse nível de maturidade, tanto em função da

insuficiência das equipes de cibersegurança dos diversos Tribunais Eleitorais no tocante à quantidade de profissionais dedicados ao tema, quanto em função da ausência de certos conhecimentos especializados por parte dessa equipe, uma vez que cibersegurança é um tema extremamente vasto e complexo, que tipicamente exige a participação conjunta de equipes multidisciplinares, internas e externas a cada órgão, para que seja obtido o sucesso desejado.

Destacamos aqui que a contratação ora pretendida tem por objetivo atender a toda a Justiça Eleitoral, englobando o TSE e todos os TREs, uma vez que os ambientes de tecnologia da informação dos TREs e do TSE possuem um razoável nível de integração, fazendo-se necessários serviços de segurança que atendam a todo esse escopo, de maneira a proteger a totalidade do ambiente tecnológico.

A necessidade dessa proteção total e integrada se materializa no direcionamento recente dos esforços em segurança cibernética da Justiça Eleitoral, em que as diretrizes vêm sendo definidas a nível nacional, a exemplo dos documentos que definem Estratégia Nacional de Cibersegurança, Arquitetura de Cibersegurança e a Estratégia Nacional de Capacitação em Cibersegurança.

Por esse motivo os serviços que hoje estão sendo contratualmente prestados tendo como escopo exclusivamente o TSE serão substituídos por esta nova contratação.

[1] - https://www.weforum.org/reports/global-cybersecurity-outlook-2023

III - A contratação consta do Plano Anual de Contratações do TSE?	[X]	**SIM. Qual Plano Orçamentário?**	[ ]	**NÃO. Justificar:**

Sim, a contratação consta do Plano de Contratações Anual - PCA 2023 (2218584), sob o código STI-007.

IV – Aquisição anterior no TSE , caso aplicável:

Não há contratações anteriores firmadas pelo TSE com escopo semelhante ao pretendido.

Como contratações correlatas, que, entretanto, não se equivalem a esta seja no escopo de serviços prestados, seja no escopo dos órgãos a serem atendidos, citamos as seguintes:

- Contrato 34/2015, firmado com a empresa Modulo Security Solutions, que, em seu item 2 contemplava a realização de serviços de consultoria em segurança da informação com base nas normas ISO 27000, que, entretanto, não contemplava o escopo aqui definido. Tal contrato já teve sua vigência expirada;
- Contrato TSE 33/2021, que cobre parcialmente a presente demanda, pois tem em seu catálogo de serviços a realização de diagnóstico/análise de maturidade com base em *frameworks* de segurança reconhecidos no mercado, porém tem como escopo apenas o TSE, não alcançando os TREs;
- Contrato TSE 32/2021 contempla ainda atividades de Análises de Vulnerabilidades de Aplicações e Testes de Invasão, que têm como escopo também apenas o TSE. Adicionalmente, não são contempla o serviço de Simulação de Ataques, que têm um escopo mais amplo, e pressupõe uma coordenação entre as atividades de ataque e as respectivas contra-atividades de defesa, além de ter como escopo de atuação apenas o TSE.

Contrato ou Nota de Empenho:	Contratos TSE nº 34/2015, 32/2021 e 33/2021
Processo SEI nº:	2016.00.000011826-8 (Contrato 34/2015), 2019.00.000009263-0 (Contratos 32 e 33/2015)
Fornecedor:	
Análise do Processo Licitatório e da Execução Contratual:	Os contratos TSE 32 e 33/2021 tiveram algumas Ordens de Serviço demandadas e executadas, tendo sido atendidas a contento, conforme comprovam seus respectivos Termos de Recebimento. Com relação ao processo licitatório, registramos que não houve questionamentos importantes com relação ao Termo de Referência que deu origem a ambos os contratos, conforme pode ser observar pela análise de seu processo de contratação, SEI n. 2019.00.000009263-0, além de não terem sido registrados quaisquer pedidos de impugnação do certame. Com relação à eventual sobreposição de escopo de atividades entre a contratação ora pretendida e os referidos contratos 32 e 33/2021, ressalta-se que as atividades previstas neste ETP, com finalidades equivalentes, estão sendo aqui delimitadas apenas para os Tribunais Regionais Eleitorais, de forma tal que apenas as atividades que não constam de nenhum dos contratos anteriores, a exemplo das simulações de ataque/defesa, terão alcance também sobre o TSE.

V - Pesquisa de mercado para identificação e análise das alternativas possíveis de solução que possam atender à necessidade:

	Soluções Identificadas	Análise da Solução
		Descrição das características principais da solução:

	Soluções Identificadas	Análise da Solução
1ª	Atendimento da demanda por meio de equipes internas da Justiça Eleitoral	Os serviços a serem prestados, de acordo com o definido pela Estratégia Nacional de Cibersegurança, são os seguintes: - Levantamento de conformidade das práticas de segurança implementadas nos Tribunais Eleitorais com base nos seguintes frameworks: - ISO 27001; - CIS Controls; - NIST CSF OBS: Cada levantamento deve ser realizado com base nas versões mais recentes de cada framework - Serviços de Análise e Exercícios de Segurança - Análises de Vulnerabilidades em Aplicações - Testes de Invasão - Simulações de Ataque/Defesa (Red Team/Blue Team) OBS: Embora a Estratégia Nacional de Cibersegurança especifique apenas os serviços de Simulações de Ataque/Defesa, é necessário que todos os tribunais eleitorais contem também com os serviços de análises de vulnerabilidades em aplicações e testes de invasão, uma vez que os resultados desses serviços fornecem os insumos para a elevação do nível de segurança do ambiente de TI de uma forma geral, e do conhecimento sobre segurança da equipe de TI em especial, elevando assim a capacidade da equipe em executar ações de defesa. - Ações de capacitação especializada em cibersegurança para as equipes de tecnologia da informação OBS: As ações de capacitação em cibersegurança específicas para as equipes técnicas serão especificadas no Plano de Capacitação em Cibersegurança da Justiça Eleitoral, que indicará sugestões de trilhas de treinamento a serem utilizadas pelos tribunais eleitorais como indicadores dos treinamentos a serem realizados. - Serviços adicionais necessários: - Mapeamento de endereços ativos na Internet e respectivos serviços habilitados; - Realização de workshops para apresetnação de temas relacionados à segurança da informação (não se caracterizam como treinamentos formais, porém apresentações sobre temas que se mostrem relevantes para a Justiça Eleitoral; Nesta Opção nº 1 todas as atividades seriam realizadas por equipes internas da Justiça Eleitoral (incluindo a possibilidade de equipes formadas também por servidores dos TREs, e não apenas do TSE).
		Vantagens e Desvantagens:

	Soluções Identificadas	Análise da Solução
		Vantagens: - Maior agilidade no atendimento às demandas, uma vez que não seria necessário aguardar a instrução e tramitação do processo de contratação - Possivelmente custos mais baixos, uma vez que as demandas seriam atendidas pela equipe já existente na Justiça Eleitoral, sem a necessidade de custos adicionais Desvantagens: - A Justiça Eleitoral ainda não possui equipe capacitada para a realização de tais atividades. Levantamento realizado em 2020 sobre a situação de cibersegurança nos Tribunais Eleitorais (constante da Estratégia Nacional de Cibersegurança), evidenciou que 19 Tribunais Eleitorais não contavam sequer com uma única pessoa dedicada ao tema em seus quadros. Essa ausência de equipes dedicadas, e mesmo de capacitação da equipe existente nos temas ora demandados, acarretaria demora na realização das atividades, e, provavelmente, baixa qualidade em boa parte das atividades necessárias. Embora tenha havido evolução na composição das equipes dedicadas à cibersegurança tanto no TSE quanto nos TREs, a Justiça Eleitoral ainda não dispõe de - Postergação de outras atividades que devam ser conduzidas pelas equipes internas OBS: O primeiro tópico apontado como desvantagem apresenta-se, na verdade, como uma restrição. A ausência de capacitação da equipe é um impeditivo à adoção desta opção. Desvantagens: - Qualidade inferior das ações de capacitação, em especial aquelas destinadas à realização de trilhas de treinamentos de formação de profissionais de segurança, uma vez que as empresas que fornecem treinamentos especializados usualmente não se dedicam às demais demandas, assim como o espectro de formação é amplo, sendo que as empresas que fornecem treinamento usualmente se especializam em determinados nichos de conhecimento, e seriam incapazes de fornecer todos os treinamentos necessários - Dificuldades na gestão e fiscalização contratual especificamente com relação às ações de capacitação, considerando-se a complexidade da coordenação e do agendamento dos diversos treinamentos a equipes técnicas de diferentes tribunais eleitorais, em função de suas lacunas específicas de conhecimento e suas disponibilidades para a participação nos cursos ofertados - Restrição da competitividade, uma vez que uma quantidade pequena de empresas tem a capacidade de prestar todos os serviços especificados.
2ª	Atendimento da demanda inteiramente por meio da contratação de uma única empresa especializada	**Descrição das características principais da solução:** Os serviços a serem prestados são os mesmos indicados na opção nº 1. Nesta Opção nº 2 todas as atividades, incluindo a realização de trilhas de treinamentos de formação de profissionais em cibersegurança, seriam realizadas por uma única empresa contratada. **Vantagens:** Vantagens: - Todos os serviços seriam prestados sob uma mesma coordenação, o que favoreceria a coerência entre as formas de atendimento das demandas e os resultados esperados para cada uma - Favorecimento da contratação de uma empresa com atuação mais ampla no ramo de segurança, o que tenderia a selecionar empresas com maior conhecimento agregado e mesmo com metodologias próprias de atuação - Simplificação da gestão e fiscalização contratual, uma vez que todos os contatos seriam acompanhados entre as mesmas equipes no TSE e na contratada **Outros Órgãos Públicos e/ou Entidades que tenham adotado solução similar:** Desconhecemos outros órgãos públicos que tenham implementado o escopo da presente demanda contando tão somente com seu quadro de servidores. **Custos estimados da solução para o TSE:** Os custos não foram estimados, uma vez que a falta de capacitação para o atendimento à demanda representa um impeditivo à sua adoção. **Outras informações relevantes:**
		Outros Órgãos Públicos e/ou Entidades que tenham adotado solução similar: Desconhecemos órgãos públicos que tenham contratado toda essa gama de serviços com uma única empresa, em função das desvantagens acima apontadas. As contratações de que tivemos ciência, contemplando objetos semelhantes ao que se pretende, estão relacionadas na opção nº 3. **Custos estimados da solução para o TSE:** Não estimamos os custos desta solução, em razão da questão do atendimento às demandas de capacitação, que se configura um impeditivo à sua adoção. **Outras informações relevantes:**
		Descrição das características principais da solução:

	Soluções Identificadas	Análise da Solução
		Os serviços a serem prestados são os mesmos indicados na opção nº 1. Nesse caso as demandas de levantamento de conformidade e demais ações técnicas seriam contratados junto a uma única empresa, tendo em vista a existência de empresas do ramo de segurança da informação/segurança cibernética que oferecem esses serviços em seu portfólio. As ações de conscientização e os treinamentos especializados em cibersegurança, entretanto, seriam contratados por cada Tribunal Eleitoral junto aos fornecedores especializados de treinamentos em cada nicho de conhecimento, de forma a melhor atender às suas necessidades específicas, bem como melhor ajustar as datas e períodos de realização de acordo com as disponibilidades de cada equipe.
		Vantagens e Desvantagens:
		Vantagens - Obtenção de melhor qualidade geral dos serviços prestados em relação à Opção nº 2, uma vez que o conjunto dos serviços demandados é ofertado por algumas empresas no mercado, e as ações de treinamentos seriam executadas por empresas especializadas em cada nicho de conhecimento. Desvantagens - Maior complexidade na contratação da prestação de serviços, uma vez que as ações de capacitação teriam que ser contratadas em blocos de temas semelhantes, ou mesmo de forma individual por tema - Restrição da competitividade, uma vez que há empresas que atuam no segmento de segurança da informação ou segurança cibernética que não são capazes de prestar todos os serviços demandados.
		Outros Órgãos Públicos e/ou Entidades que tenham adotado solução similar:
3ª	Contratação dos serviços de levantamento de conformidade e demais ações técnicas junto a uma mesma empresa, e contratação de ações de conscientização capacitação especializada junto aos diversos fornecedores do mercado (em procedimentos licitatórios distintos), de acordo com as respectivas especializações	

	Soluções Identificadas	Análise da Solução
		- Banco Central: - Contrato: 50904/2019 - Objeto: prestação de serviços de consultoria em segurança cibernética para avaliações de resiliência cibernética e risco cibernético - BNDES: - Contrato: 367/2019 - Objeto: Serviço de testes independentes de penetração e análise de segurança para a realização de até 4 (quatro) testes - Conselho da Justiça Federal: - Contrato: 8/2020 - Objeto: Serviços de Segurança da Informação nº 1. a) Serviço de operação e atendimento a requisições. b) Serviço de gestão de incidentes de segurança (CSIRT - Blue Team). c) Serviço de gestão de vulnerabilidades. d) Serviço de monitoramento e visibilidade de ataques cibernéticos. e) Serviço de orquestração, automação e resposta de segurança (SOAR). f) Serviço de testes de invasão (Red Team). - Conselho Nacional de Justiça: - Pregão: 03/2021 - Objeto: Serviços Gerenciados de Segurança da Informação • Serviço de administração, operação e manutenção e atendimento a requisições • Serviço de gestão de vulnerabilidades • Serviço de gestão de incidentes de segurança (CSIRT - Blue Team) • Serviço de monitoramento e visibilidade de ataques cibernéticos • Serviços de testes de invasão (Red Team)
4ª	Contratação dos serviços de levantamento de conformidade e demais ações técnicas em lotes compostos por serviços de competências similares, e contratação de ações de conscientização capacitação especializada junto aos diversos fornecedores do mercado (em	**Descrição das características principais da solução** Os serviços seriam prestados nos moldes indicados na opção nº 1. Nesse caso as demandas de levantamento de conformidade e demais ações técnicas seriam subdivididos em lotes distintos, com os itens agrupados por competências similares, tendo em vista a existência de empresas do ramo de segurança da informação/segurança cibernética que prestam apenas partes dos serviços especificados. As ações de conscientização e os treinamentos especializados em cibersegurança, entretanto, seriam contratados por cada Tribunal Eleitoral junto aos fornecedores especializados de treinamentos em cada nicho de conhecimento, de forma a melhor atender as suas necessidades específicas, bem como melhor ajustar as datas e períodos de realização de acordo com as disponibilidades de cada equipe. **Vantagens e Desvantagens;** Vantagens - Aumento da competitividade, uma vez que há empresas no mercado que prestam apenas parte dos serviços especificados, com manutenção da boa qualidade geral dos serviços prestados, em função da especialização dos possíveis competidores. - Possível incremento da qualidade dos serviços agrupados em cada lote, em razão da especialização dos competidores que participem da licitação. Desvantagens - Maior complexidade na contratação da prestação de serviços, uma vez que as ações de capacitação teriam que ser contratadas em blocos de temas semelhantes, ou mesmo de forma individual por tema. **Custos estimados da solução para o TSE:** Os custos são estimados em **R$ 12.085.929,85**. (conforme detalhamento no item VIII) - Perda de um padrão de execução único dos serviços em relação à Opção nº 3, pois naquela opção, todos os serviços (à exceção dos serviços de conscientização e treinamentos especializados) seriam prestados por uma única empresa. **Outras informações relevantes:** Não há **Outros Órgãos Públicos e/ou Entidades que tenham adotado solução similar:**

Soluções Identificadas Soluções Identificadas (ambientes tecnológicos distintos), de acordo com as respectivas especializações	**Análise da Solução** Aqui consideramos a mesma relação de órgãos indicada na Opção 3, uma vez que todos os contratos identificados coincidem apenas parcialmente com a contratação ora pretendida: - Banco Central: - Contrato: 50904/2019 - Objeto: prestação de serviços de consultoria em segurança cibernética para avaliações de resiliência cibernética e risco cibernético - BNDES: - Contrato: 367/2019 - Objeto: Serviço de testes independentes de penetração e análise de segurança para a realização de até 4 (quatro) testes - Conselho da Justiça Federal: - Contrato: 8/2020 - Objeto: Serviços Gerenciados de Segurança da Informação a) Serviço de operação e atendimento a requisições. b) Serviço de gestão de incidentes de segurança (CSIRT - Blue Team). c) Serviço de gestão de vulnerabilidades. d) Serviço de monitoramento e visibilidade de ataques cibernéticos. e) Serviço de orquestração, automação e resposta de segurança (SOAR). f) Serviço de testes de invasão (Red Team). - Conselho Nacional de Justiça: - Pregão: 03/2021 - Objeto: Serviços Gerenciados de Segurança da Informação • Serviço de administração, operação e manutenção e atendimento a requisições • Serviço de gestão de vulnerabilidades • Serviço de gestão de incidentes de segurança (CSIRT - Blue Team) • Serviço de monitoramento e visibilidade de ataques cibernéticos • Serviços de testes de invasão (Red Team)
	Custos estimados da solução para o TSE:
	Os custos são estimados em **R$ 12.085.929,85**. (conforme detalhamento no item VIII)
	Outras informações relevantes:
	Não há

VI - Detalhamento da solução que, por entendimento do(s) signatário(s) deste documento, melhor atenderá à necessidade objeto deste Estudo:

A opção que melhor atende às necessidades de objetivos da contratação pretendida, no entendimento desta Equipe de Planejamento da Contratação, é a Opção nº 4 - "Contratação dos serviços de levantamento de conformidade e demais ações técnicas em lotes agrupados por competências similares, e contratação de ações de conscientização capacitação especializada junto aos diversos fornecedores do mercado, de acordo com as respectivas especializações", pelas seguintes razões:

- A opção nº 1 não se mostra viável, conforme observação registrada na relação de suas desvantagens:

  "O primeiro tópico apontado como desvantagem apresenta-se, na verdade, como uma restrição. A ausência de capacitação da equipe é um impeditivo à adoção desta opção."

- A opção nº 2 apresenta desvantagem, equivalentes à:

  "Qualidade inferior das ações de capacitação, em especial aquelas destinadas à realização de trilhas de treinamentos de formação de profissionais de segurança, uma vez que as empresas que fornecem treinamentos especializados usualmente não se dedicam às demais demandas, assim como o espectro de formação é amplo, sendo que as empresas que fornecem treinamento usualmente se especializam em determinados nichos de conhecimento, e seriam incapazes de fornecer todos os treinamentos necessários"

- A opção nº 3 também apresenta uma desvantagem importante:

  "Restrição da competitividade, uma vez que há empresas que atuam no segmento de segurança da informação ou segurança cibernética que não são capazes de prestar todos os serviços demandados"

Assim, e Equipe de Planejamento da Contratação entende que a Opção nº 4 é a mais adequada, uma vez que, em razão dos valores envolvidos na contratação, entendemos que seja importante priorizar a competitividade, ainda que à custa de uma possível perda de padrão entre a prestação dos serviços relativos aos diferentes lotes.

A opção escolhida se caracteriza pela execução de serviços especializados de segurança cibernética para todos os Tribunais Eleitorais, de forma que o TSE possa ter em mãos um conhecimento integrado sobre a situação da Justiça Eleitoral. Esses serviços especializados são subdivididos nos seguintes itens:

1) Realização de Diagnóstico/Análise de maturidade em cibersegurança em todos os tribunais da Justiça Eleitoral

A organização dos recursos e atividades de segurança da informação e de segurança cibernética é objeto de sistematização por alguns *frameworks* amplamente reconhecidos pelo mercado, e a realização de diagnóstico ou análise de maturidade de uma organização a partir desses *frameworks* fornece uma boa fotografia de seu estado atual, permitindo uma melhor organização dos esforços a serem empreendidos para que seja alcançado o nível de segurança adequado ou desejado.

Dentre os *frameworks* reconhecidos pelo mercado destacam-se os abaixo relacionados, que possuem enfoques distintos entre si, sendo úteis, portanto, para identificar a situação e direcionar os esforços referentes a diferentes aspectos de segurança da informação e segurança cibernética:

- ISO 27001:

  Definição: conforme definido no item 1 da Norma – Escopo:

  > *"Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Os requisitos definidos neste Norma são genéricos e são pretendidos para serem aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza. A exclusão de quaisquer dos requisitos especificados nas Seções 4 a 10 não é aceitável quando a organização busca a conformidade com esta norma."*

  A norma ISO 27001 é um dos padrões mundialmente aceitos como boas práticas de organização da segurança da informação em uma instituição, e oferece inclusive mecanismos de certificação, por meio de empresas acreditadas, que atestem que a instituição efetivamente estabeleceu um sistema de segurança da informação e o implementa conforme estabelecido.

  Não será objeto dos serviços a serem contratados, entretanto, a preparação dos tribunais eleitorais para a certificação na norma ISO 27001, e mesmo a certificação em si, mas somente a realização de análises de conformidade de forma a identificar a situação atual e direcionar esforços para que cada tribunal eleve seu padrão de segurança da informação de acordo com seus objetivos estabelecidos.

- NIST CSF (Cyber Security Framework):

  Definição: Conforme trechos extraídos da tradução do NIST CSF elaborada pela US Chamber of Commerce:

  > *"o Guia oferece uma taxonomia e mecanismos comuns para que as organizações:*
  >
  > *1) Descrevam sua situação atual no que tange à segurança cibernética*
  >
  > *2) Descrevam seus objetivos no que tange à segurança cibernética*
  >
  > *3) Identifiquem e priorizem oportunidades de aperfeiçoamento dentro*
  >
  > *do contexto de um processo contínuo e reproduzível*
  >
  > *4) Avaliem seus progressos frente aos objetivos*
  >
  > *5) Comuniquem-se com stakeholders internos e externos sobre os riscos*
  >
  > *apresentados na atual segurança cibernética.*
  >
  > *...*
  >
  > *Para atender às necessidades específicas de segurança cibernética inerentes a cada organização, há uma grande variedade de maneiras de utilizar o Guia. A decisão*
  >
  > *sobre como aplicá-lo é responsabilidade da organização implementadora. Por exemplo, uma organização pode optar por utilizar os Níveis de Implementação da*
  >
  > *Estrutura Básica para articular as práticas de gerenciamento de risco previstas. Uma outra organização pode usar as cinco funções da Estrutura Básica para analisar todo*
  >
  > *seu portfólio de gerenciamento de riscos. Essa análise pode ou não contar com orientações complementares mais detalhadas, como catálogos de controles. Às*
  >
  > *vezes há discussão sobre "compliance" com o Guia, sendo que o mesmo tem utilidade como uma estrutura e linguagem para organizar e apresentar o programa*
  >
  > *de compliance de acordo com os requisitos de segurança cibernética da própria organização. No entanto, a variedade de maneiras pelas quais o Guia pode ser*
  >
  > *usado por uma organização significa que frases como "compliance com o Guia" podem ser confusas e significar algo muito diferente para os vários stakeholders*
  >
  > *envolvidos no processo."*

  Conforme se depreende do texto acima, a multiplicidade de opções de utilização do guia referente ao NIST CSF não permite a existência de mecanismos oficiais de certificação de conformidade.

  Assim, para os fins da contratação pretendida, as análises de conformidade a serem realizadas com base no NIST CSF terão como base a totalidade do conteúdo de seu item "Estrutura Básica" e deverão identificar o seu "Nível de Implementação".

  Conforme sugerido pelo próprio guia do NIST CSF, as avaliações realizadas serão utilizadas para dar suporte a:

  - Fazer escolhas sobre como diferentes partes da operação de segurança cibernética devem influenciar a seleção dos Níveis de Implementação desejados
  - Avaliar a abordagem da organização quanto ao gerenciamento de riscos de segurança cibernética, determinando os Níveis de Implementação Atuais
  - Priorizar os resultados de segurança cibernética através do desenvolvimento de Avaliações Desejadas
  - Determinar o grau em que cada etapa específica de segurança cibernética alcança os resultados desejados de segurança cibernética, analisando Avaliações Atuais, e
  - Avaliar o grau de implementação de catálogos de controles ou orientação técnica listados como Referências Informativas

- CIS Controls:

Definição: De acordo com o documento CIS Controls v7.1, em tradução livre:

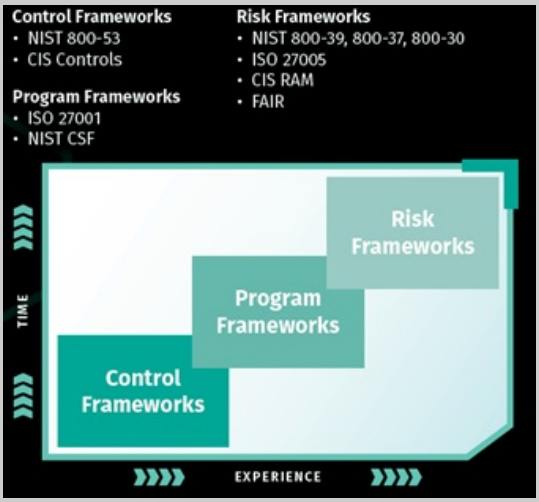
> *"Os CIS Controls é um conjunto priorizado de ações que formam uma coleção de melhores práticas de defesa em profundidade que mitigam os ataques mais comuns contra sistemas e redes de computador. São desenvolvidos por uma comunidade de especialistas em TI que aplicam sua experiência em primeira mão em atividades de defesa cibernética para elaborar essas melhores práticas aceitas globalmente. Tais especialistas são oriundos de uma grande amplitude de áreas de atuação tais como varejo, manufatura, saúde, educação, governo, defesa e outras."*

O CIS Controls vem efetivamente sendo utilizado como referência por diversos setores do mercado, tendo sido adotado como base para a Estratégia Nacional de Cibersegurança do Poder Judiciário (ENSEC-JUD), bem como para recentes ações de auditoria conduzidas pelo TCU, tais como seu Acompanhamento de Segurança Cibernética(1), onde esclarece que *"os critérios utilizados para subsidiar a elaboração deste questionário foram livremente adaptados a partir do julgamento profissional da equipe de auditores do TCU sobre a versão 8 do framework desenvolvido pelo Center for Internet Security (CIS)".*

Assim como no caso do NIST CSF, o CIS Controls também não possui mecanismos de certificação de conformidade. Assim, para os fins da contratação pretendida, as análises de conformidade a serem realizadas com base no CIS Controls terão como base a totalidade do conteúdo de sua versão 8 (ou mais recente, se assim for solicitado pelos tribunais eleitorais).

- Relacionamento entre os *frameworks*:

Conforme registrado inicialmente, os *frameworks* citados possuem enfoques distintos entre si. A norma ISO 27001 e o NIST CSF são exemplos de *frameworks* de Programas de Segurança da Informação, enquanto o CIS Controls é um exemplo de *framework* de Controles de Segurança, podendo ser utilizados em conjunto para a estruturação de um programa de segurança mais abrangente e detalhado. A figura abaixo, extraída do poster de divulgação do CIS Controls v7(2) ilustra essa relação:



Observa-se que a figura sugere que em estágios iniciais de experiência da organização sejam adotados *frameworks* de Controles, como é o caso do TSE, que adota o CIS Controls desde 2019, e que, com o avanço da experiência e maturidade das organizações, sejam adotados em sequência *frameworks* de Programas de Segurança e de Gestão de Riscos.

Assim, a presente contratação busca garantir que, além da análise externa quanto à adoção de controles de segurança, exista também possibilidade de que sejam realizados diagnósticos de conformidade externos com base também nos *frameworks* de Programas de Segurança NIST CSF e ISO 27001, de forma a viabilizar que a evolução dos esforços em segurança seja moldada a partir de um ou de ambos os *frameworks.*

2) Realização de simulações de ataque, por meio de Red Teams (equipes de ataque) externos, e Blue Teams (equipes de defesa) da Justiça Eleitoral

A realização de simulações de ataque e defesa buscam primordialmente avaliar os conhecimentos e habilidades da equipe interna de defesa cibernética relativos à reação a ataques que venham a ser realizados contra o ambiente de TI. A própria natureza desses exercícios pressupõe que já haja alguma organização das equipes internas para o monitoramento do cenário de segurança e consequente reação a ataques.

O *framework* CIS Controls, tanto em sua versão 7.1 quanto em sua versão 8, posiciona os testes de invasão externos e exercícios de ataque/defesa como o último dos controles (nº 20 no CIS Controls 7.1 e nº 18 no CIS Controls v8), e em ambos prevê como de realização obrigatória apenas para organizações de porte médio e grande (Implementation Groups 2 e 3).

Em razão dessas características, é entendimento da Equipe de Planejamento da Contratação que os serviços de simulações de ataque e defesa previstos na Estratégia Nacional de Cibersergurança, avaliados à luz da Arquitetura de Cibersegurança definida como produto dessa estratégia (Processo 2021.00.000007383-0, documento 1778308), exigem o cumprimento dos pré-requisitos dois outros serviços: Testes de Invasão e Análises de Vulnerabilidades

Dessa forma, a composição de serviços deste item seria a seguinte:

- Análise de Vulnerabilidade de Aplicações, composta por:
  - Análise Estática de Código-fonte (SAST – Static Application Security Testing)
    - Tem por objetivo analisar o código-fonte quanto a técnicas inseguras de progrmação
  - Análise de Bibliotecas de Terceiros (SCA – Software Composition Analysis)
    - Tem por objetivo analisar as bibliotecas de terceiros utilizadas nos projetos de software, identificando vulnerabilidades conhecidas associadas a essas bibliotecas
  - Análise Dinâmica de Aplicações (DAST – Dynamic Application Security Testing)
    - Tem por objetivo analisar a aplicação em execução, identificando problemas de segurança associados à sua utilização efetiva
- Mapeamento de Endereços IP ativos na Internet e respectivos serviços habilitados
  - Tem por objetivo a identificação do ambiente de TI de cada tribunal eleitoral identificável por um eventual atacante a partir da Internet, o que representa o ambiente mais vulnerável a ataques externos
- Teste de Invasão
  - O teste de invasão busca identificar, a partir do ponto de vista de um atacante, as fraquezas de uma determinada aplicação ao ambiente de TI, e explorá-las de forma a determinar até onde um atacante pode chegar e quais processos de negócios ou dados podem ser afetados pela exploração dessa vulnerabilidade
- Simulações de ataque/defesa
  - As simulações de ataque/defesa, também conhecidos como exercícios de “Red Team”, são semelhantes aos testes de invasão em que as vulnerabilidades são exploradas, porém com foco na simulação de Táticas, Técnicas e Procedimentos (TTPs) de atacantes específicos para avaliar como o ambiente de uma empresa, incluindo sua equipe de defesa, resistiria a um ataque de um adversário específico ou uma categoria de adversários. Tais simulações, portanto, requerem uma coordenação entre as ações de ataque/defesa, e uma posterior avaliação das ações executadas pela equipe de defesa, de forma a identificar lacunas de habilidades e conhecimentos, fornecendo assim subsídio para ações de capacitação da equipe, revisão de procedimentos, e providências semelhantes.

Observação:

Com relação à "contratação de ações de conscientização capacitação especializada", destacamos que a recomendação para sua contratação junto aos diversos fornecedores do mercado (em procedimentos licitatórios distintos), de acordo com as respectivas especializações, consta como recomendação da Estratégia Nacional de Capacitação em Cibersegurança, formalizada por meio do processo SEI n. 2021.00.000010960-6, conforme trecho abaixo transcrito:

> *"A presente Estratégia de Capacitação prevê uma extensa gama de ações que perpassam diversos temas, e que devem ser adotadas pelos diversos Tribunais Eleitorais.*
>
> *Essas características impõem importantes desafios à sua implementação, seja com relação à oferta de treinamentos pelos diversos fornecedores disponíveis no mercado, que dificilmente terão a capacidade de individualmente fornecerem todos os cursos propostos, seja com relação à composição das equipes de TI dos diversos tribunais eleitorais, que impõe diferentes restrições para que essas equipes participem das ações de capacitação, quanto à quantidade de treinamentos de que possam participar por ano, e quanto à efetiva disponibilidade de agendas em datas específicas.*
>
> *Assim, propõe-se que:*
> *• O Tribunal Superior Eleitoral elabore Programa de Conscientização, contando com o apoio do contrato TSE 33/2021.*
> *• o Tribunal Superior Eleitoral coordene a adaptação para âmbito nacional dos treinamentos já elaborados pelo TRE-MG e TRE-PE, voltados à conscientização do público interno em geral;*
> *• o GT-SI (Grupo de Trabalho em Segurança da Informação) seja responsável pela identificação e disponibilização, no Portal de Segurança da Informação (em elaboração), de cursos EaD, panfletos digitais e outras peças de conscientização que já tenham sido produzidas por tribunais eleitorais ou por entidades nacionais (como o CNJ, Cert.br, etc.) com relação à segurança da informação;*
> *• os Tribunais Regionais Eleitorais sejam responsáveis pelas contratações dos demais treinamentos previstos neste Plano Nacional de Capacitação, observando as prioridades sugeridas e adaptando-as às suas realidades específicas*
> *• o Tribunal Superior Eleitoral realize o registro e acompanhamento das ações de capacitação em segurança da informação ou cibersegurança realizadas pelos Tribunais Regionais."*

Com efeito, a Justiça Eleitoral já iniciou ações nesse sentido, a exemplo da contratação conjunta de plataforma de conscientização em segurança que foi realizada por meio de licitação capitaneada pelo TRE-ES, que resultou na Ata de Registro de Preços nº 04/2022 daquele tribunal, sobre a qual diversos tribunais eleitorais já efetivaram contratações, a exemplo do contrato TSE nº 105/2022.

Dessa forma, esses serviços não serão contemplados no escopo da presente contratação.

[1] - https://contas.tcu.gov.br/pesquisas/index.php/472879?token=OG3VHhh9tob7M6l&lang=pt-BR

[2] - https://www.cisecurity.org/white-papers/cis-controls-v7-poster/

VII - Quantidades a serem contratadas e justificativas fundamentadas:

1) Realização de Diagnóstico/Análise de maturidade em cibersegurança em todos os tribunais da Justiça Eleitoral

- Até dois levantamentos por ano, para o conjunto dos tribunais eleitorais, para até dois dos frameworks definidos (ISO 27001, NIST CSF e CIS Controls), sendo um levantamento inicial e um possível levantamento de acompanhamento das melhorias;
    - Isto equivale a um máximo de quatro levantamentos por ano.
- Até quinze workshops sobre temas relacionados à segurança da informação, de interesse do TSE, de um ou mais TREs, ou de toda a Justiça Eleitoral
    - Foi estimado um número máximo de 15 workshops por ano, o que equivale a um workshop por mês, e três workshops adicionais para acomodar eventuais necessidades, em uma estimativa empírica sobre a quantidade máxima de demandas por toda a Justiça Eleitoral, devido à ausência de um referencial deste tipo de demanda.

2) Realização de simulações de ataque, por meio de Red Teams (equipes de ataque) externos, e Blue Teams (equipes de defesa) da Justiça Eleitoral

As estimativas abaixo referem-se à execução em um período de um ano.

- Análises de Vulnerabilidades de Aplicações
    - Quantidades estimadas a partir do levantamento realizado junto aos TREs, materializado no documento 1934145.
        - Os quantitativos adotados equivalem a um terço das quantidades de aplicações indicadas pelos TREs, considerando-se a necessidade de disponibilidade das equipes dos TREs para o tratamento das vulnerabilidades eventualmente detectadas pelas análises;
        - Para os casos em que as quantidades de aplicações indicadas pelos TREs eram "0" ou "1", adotamos o quantitativo máximo de 2 análises de vulnerabilidade, de forma a acomodar o surgimento de novas aplicações de complexidade baixa, média ou alta que necessitem ser submetidas à análise de vulnerabilidades.
- Mapeamento de Endereços IP ativos na Internet e respectivos serviços habilitados
    - Faixa de até 8 endereços IP: 2
    - Faixa de até 16 endereços IP: 34
    - Faixa de até 32 endereços IP: 14
    - Faixa de até 64 endereços IP: 10
    - Faixa de até 128 endereços IP: 4
    - Faixa de até 256 endereços IP: 4
        - Quantidades estimadas a partir do levantamento realizado junto aos TREs, materializado no documento 1934145.
        - As quantidades adotadas são referentes a até dois mapeamentos para cada faixa de endereços IP por ano.
- Testes de invasão
    - 5 testes de invasão por TRE
    - 10 testes de invasão para o TSE
    - Total: 145 testes
- Exercícios de Ataque/Defesa
    - Até 640 horas a serem consumidas pelo TSE (equivalente a 80 dias úteis de trabalho de um único especialista)
    - Até 160 horas a serem consumidas por cada TRE (equivalente a 20 dias úteis de trabalho de um único especialista)
        - Observações:
            - É esperado que cada exercício de Ataque/Defesa demande mais de um especialista;
            - Exercícios de ataque/defesa são complexos por natureza de forma que recomendamos a execução de até dois exercícios por ano, sendo um para a avaliação inicial da postura de segurança do ambiente e da equipe responsável pela segurança cibernética, e eventualmente um segundo teste anual, para avaliar a evolução dessa postura. Está sendo prevista uma quantidade de horas superior para o TSE, uma vez que o ambiente de TI é mais complexo do que os dos TREs, e uma maior quantidade de horas disponíveis permite a realização de exercícios de ataque/defesa que abordem diferentes aspectos do ambiente do TSE.
- Parecer especializado sobre softwares de prateleira ou serviços disponibilizados da Internet
    - Trata-se da emissão de pareceres especializados sobre aspectos de segurança de softwares de prateleira (inclusive de código aberto - *opensource)* ou serviços que algum tribunal eleitoral tenha interesse em adotar
        - Considerando que, ainda que a demanda surja em um tribunal eleitoral específico, cada parecer será de interesse de toda a justiça eleitoral, estimamos a demanda em até dois pareceres para cada tribunal
- Definição de padrões de configuração seguros para ativos de Tecnologia da Informação
    - Considerando que o TSE possui um ambiente de TI mais complexo do que os dos TREs, e que cada padrão de configuração segura será disponibilizado a todos os tribunais eleitorais, as demandas foram estimadas da seguinte forma:
        - Até 10 definições de padrões seguros demandadas pelo TSE
        - Até 2 definições de padrões seguros demandadas pelos TREs

Observação: O Termo de Referência irá prever que os serviços deverão ser demandados por meio de Ordens de Serviço, entretanto, sem garantia mínima de execução.

3) Apuração de incidente de segurança

A Justiça Eleitoral deve contar com o apoio especializado para a apuraç

para o consumo desses serviços é a seguinte:

- Até 320 horas a serem consumidas pelo TSE (equivalente a 40 dias úteis de trabalho de um único especialista)
- Até 80 horas a serem consumidas por cada TRE (equivalente a 10 dias úteis de trabalho de um único especialista)
    - Observações:
        - É esperado que cada apuração de incidente de segurança demande mais de um especialista;
        - Está sendo prevista uma quantidade de horas superior para o TSE, uma vez que o ambiente de TI é mais complexo do que os dos TREs, o que teoricamente possibilita que incidentes afetem uma quantidade maior de ativos no ambiente do TSE.

VIII - Valor estimado da contratação:

A presente contratação já foi submetida à estimativa de preços de mercado com base na versão do Termo de Referência (2056715) imediatamente anterior ao parecer da Assessoria Jurídica (2322208).

Considerando-se que as recomendações exaradas pela Assessoria Jurídica não provocam alterações na especificação dos serviços, e, consequentemente, na estimativa de preços, indicamos que o valor estimado para a contratação é o resultado da estimativa de preços já realizada, materializada na Informação SECGA/CODAQ/SAD nº 815/2022 (2328077), o que equivale a **R$ 12.085.929,85**.

Destacamos que este é o custo máximo da contratação, uma vez que todos os serviços contam com uma quantidade de demandas máxima, não havendo, entretanto, garantia de demanda mínima por exercício contratual. As demandas serão efetivamente formalizadas de acordo com as necessidades de cada tribunal eleitoral, e da disponibilidade de suas equipes em acompanharem a realização dos serviços e tratarem os respectivos resultados.

IX - A solução é divisível?	[X]	**SIM.**	[ ]	**NÃO.**	**Justificar:**

A solução está sendo indicada como divisível nos termos da Opção nº 4, onde os serviços serão agrupados de acordo com suas especializações em lotes independentes.

A Lei 8.666/1993, em seu Art. 23, §1º, define que "§ 1º As obras, serviços e compras efetuadas pela Administração serão divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala".

Analisando-se a divisibilidade de acordo com a definição da lei:

a) é tecnicamente viável dividir a solução?

Sim, de acordo com os lotes propostos na Opção nº 4. Tal divisão inclusive decorreu da avaliação das propostas técnico-comerciais que recebemos por ocasião do levantamento da estimativa de preços para a primeira versão do Termo de Referência, que se baseava em um lote único, e tinha por objetivo selecionar uma única empresa com alta especialização em segurança da informação e segurança cibernética, que tivesse expertise para prestar a totalidade dos serviços demandados.

b) é economicamente viável dividir a solução?

Sim. Tal conclusão também se apoia no levantamento da estimativa de preços para a primeira versão do Termo de Referência, que se baseava em um lote único.

c) não há perda de escala ao dividir a solução?

Não, uma vez que não se trata da aquisição ou contratação de bens ou serviços produzidos em série, mas sim serviços de contornos variáveis a depender do perfil do ambiente tecnológico e das demandas de cada Tribunal Eleitoral.

d) há o melhor aproveitamento do mercado e ampliação da competitividade ao dividir a solução?

Sim, nos termos da Opção nº 4, que traz um balanceamento entre ampliação da competitividade e manutenção de um padrão e coerência na prestação de serviços de maior similaridade

X - Resultado(s) esperado(s) com a contratação:

Identificação do nível de maturidade dos diversos Tribunais Eleitorais com relação à cibersegurança e segurança da informação, o que será utilizado como insumo para evoluir a Estratégia Nacional de Cibersegurança da Justiça Eleitoral.

Avaliação do nível de segurança das principais aplicações e ambientes de TI dos Tribunais Eleitorais, permitindo assim a correção das eventuais vulnerabilidades identificadas e a evolução dos conhecimentos e habilidades de defesa das equipes internas.

XI - Critérios e práticas de sustentabilidade aplicáveis a solução escolhida:

Orientações obtidas a partir de consulta ao sistema "Painel Gerencial - Critérios de Sustentabilidade", tendo sido identificada a Informação AGES/GAB-DG nº 84/2020 (documento n. 1313067), referente à contratação de Serviços de Análise em Segurança da Informação, análoga a esta que agora se instrui.

- Os produtos desenvolvidos pela contratada serão entregues ao tribunal em arquivos de computador, em formatos compatíveis com o Microsoft Office ou com o padrão PDF, ou em formatos específicos para produtos que devam ser visualizados em aplicações distintas, formatos esses a serem previamente acordados entre a contratada e o TSE;
    - Somente será permitida a entrega de produtos impressos em caso de solicitação por parte do tribunal, ou em caso de sugestão da contratada acatada pelo tribunal;
- 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.
- 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.

XII - Restrições internas de caráter técnico, operacional, regulamentar, financeiro e orçamentário, que possam dificultar a implementação da solução eleita:

A execução dos serviços de Análise de Vulnerabilidades de Aplicações em princípio será executado remotamente, a partir da disponibilização de recursos de virtualização para que a contratada remotamente instale suas ferramentas e realize os testes necessários.

Entretanto eventuais dificuldades que podem advir desta forma de atuação serão reavaliadas por ocasião da elaboração do Termo de Referência, havendo a possibilidade de que se especifique que tais serviços devam ser executados presencialmente, o que pode encarecê-los.

XIII - Observações: