

PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN, Quadra 02 Bloco E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3866 - <https://www.iti.gov.br>

ESTUDO TÉCNICO PRELIMINAR

Contratação de Serviços de Operação de Infraestrutura para o ambiente de Assinaturas Eletrônicas Avançadas do ITI

Processo Administrativo nº 00100.003688/2021-94

Histórico de Revisões

Data	Versão	Descrição	Autor
08/03/2022	0.1	Versão inicial do documento.	Marcelo Fenoll Ramal
29/03/2022	1.0	Ajustes finais	Marcelo Fenoll Ramal
09/06/2022	1.1	Revisão conjunta COLIC	Marcelo Fenoll Ramal e Ornel Costa de Azevedo

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

<p>A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da solução para de serviços técnicos especializados de operação de infraestrutura de TIC, exclusivos para o ambiente de Assinaturas Eletrônicas Avançadas do ITI, com monitoramento por meio de NOC (Network Operations Center/Centro de Operações de Rede) e SOC (Security Operations Center/Centro de Operações de Segurança).</p> <p>Entende-se por "operação de infraestrutura de TIC" a prestação de serviços técnicos que estão relacionados à segurança da informação, intercomunicação e rede de comunicação de dados, banco de dados, servidores de rede, sistemas operacionais, sistemas de backup, recursos de armazenamento de dados, monitoramento e gerenciamento operacional.</p> <p>Entende-se por "NOC" a implantação de um sistema composto por hardware, software e recursos humanos organização para o monitoramento e gerenciamento de uma rede de computadores. Informações como níveis de serviço, uso de recursos computacionais, indicativos de criticidade ou indisponibilidade são utilizados para identificar riscos (preventivo) e problemas (reativo) e iniciar o tratamento das ações necessárias para adequação do ambiente.</p> <p>Entende-se por "SOC" a implantação de um sistema composto por hardware, software e recursos humanos organização para o monitoramento e gerenciamento de segurança uma rede de computadores. Informações como tentativas de ataque, alertas de problemas de segurança identificados por fabricantes, indicativos de invasão ou acesso indevido são utilizados para identificar riscos (preventivo) e problemas (reativo) e iniciar o tratamento das ações necessárias para adequação do ambiente.</p> <p>Enquanto o fornecimento de hardware e software dos ambientes de NOC e SOC serão de obrigação do ITI, os recursos humanos (competência técnica-operacional) serão de responsabilidade da contratada. Desta forma, todos os requisitos, serviços, produtos (artefatos) e atribuições descritos neste TR e seus anexos são de inteira responsabilidade da contratada, salvo aqueles explicitamente definidos como obrigações compartilhadas.</p> <p>Não fazem parte do escopo desta contratação: a) os serviços de atendimento aos usuários (suporte níveis 1 a 3); b) a manutenção de sistemas de informação (relativos à fábrica de software e similares); c) os serviços de Operação de Infraestrutura para a área meio de TI do ITI; d) os serviços de Operação de Infraestrutura para o ICP-Brasil.</p> <p>Todos e quaisquer equipamentos e serviços do ITI eventualmente compartilhados com a STI de "Chaves e Assinaturas Avançadas" fazem parte do escopo dos serviços contratados de operação de infraestrutura.</p> <p>Referência: Art. 11 da IN SGD/ME nº 1/2019.</p> <p>Este estudo está registrado no sistema de ETP Digital sob o número 6/2022</p>
--

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. Identificação das necessidades de negócio

1	Monitorar e manter operante, em regime permanente e ininterrupto, os sistemas e equipamentos (software e hardware) responsáveis pelos serviços de assinaturas avançadas do ITI.
2	Contratar serviços técnicos especializados para operação de infraestrutura específica (relacionada aos serviços finalísticos do ITI para o provimento de Assinatura Eletrônica Avançada), contemplando os seguintes serviços de TIC: sustentação, prevenção, manutenção e operação de ambiente corporativo de TI, em formato de operação de Centro de Dados, que efetuem o monitoramento proativo, preventivo e imediata correção de falhas de segurança, problemas de configuração, defeitos e outros eventos que afetem a qualidade, segurança e disponibilidade dos serviços de Assinatura Eletrônica Avançada.
3	Garantir que o ambiente sustentado atenda aos requisitos de performance, qualidade, integridade e disponibilidade da informação, dos serviços e das soluções de TIC relacionadas ao ambiente de assinatura avançada.
4	No caso de eventos de interrupção de serviços, assegurar a restauração tempestiva da operação normal dos serviços de Assinatura Avançada, como mínimo de impacto nos processos de negócios do ITI, obedecendo os padrões e níveis mínimos de serviço.
5	Manter o nível adequado de segurança, integridade e consistência dos dados manipulados e armazenados no datacenter do ITI.
6	Resolver problemas respeitando os níveis mínimos de serviço, de modo que se amplie o nível de satisfação quanto aos serviços prestados.
7	Diminuir os eventos de risco e problemas operacionais, por meio de ações proativas e de melhoria contínua do ambiente.
8	Aumentar a confiabilidade do sistema, diminuindo progressivamente o tempo de interrupção dos serviços.
9	Disponibilizar técnicos em regime híbrido (preferencialmente remoto) que efetuem o monitoramento contínuo e ininterrupto de todo o ambiente tecnológico relacionado ao serviço de assinatura eletrônica avançada, bem como das ações de manutenção. O atendimento presencial será requerido apenas para atividades físicas-operacionais de manutenção.
10	Atuar em conjunto com outros prestadores de serviço quando da instalação e/ou substituição de peças, equipamentos, servidores, máquinas, ativos de rede e outros relacionados ao ambiente de TIC, de forma a manter a qualidade, performance e segurança, bem como os níveis de serviço.

11	Os locais para atuação remota dos profissionais serão os seguintes: <ul style="list-style-type: none"> PR – Localizado no anexo do Palácio do Planalto, Brasília, DF; UFSC – Localizado em Florianópolis/SC. <p>O acesso físico eventual se dará exclusivamente no sítio localizado em Brasília/DF.</p>
12	Este planejamento de contratação deve estar alinhado com o modelo de contratação de serviços de operação de infraestrutura e de atendimento de usuários de TIC do SISP/ME, disponível no endereço https://www.gov.br/governodigital/pt-br/contratacoes/modelo-de-contratacao-de-servicos-de-operacao-de-infraestrutura-e-de-atendimento-a-usuarios-de-tic , e com a Portaria SGD/ME no 6.432, de 15 de junho de 2021, disponível em https://www.gov.br/governodigital/pt-br/contratacoes/portaria-sgd-me-no-6-432-de-15-de-junho-de-2021 .
13	Transformar atividades humanas repetitivas de manutenção por atividades automatizadas, como por exemplo pelo uso de ferramentas de automação robótica de processos (RPA).
14	Implantar ferramentas de monitoramento de infraestrutura de TI (ITIM) para o monitoramento da saúde da TI em tempo real.
15	Criar um ambiente de monitoramento do tipo NOC, utilizando a estrutura física da empresa prestadora de serviço.
16	Capacitar prestadores da contratada nos assuntos técnicos específicos do ITI para o serviço de Assinaturas Avançadas.
17	Garantir o acesso físico ao menos a dois prestadores da empresa contratada ao centro de dados do ITI. Este procedimento requer validações de segurança especiais devido a criticidade da solução.

1.2. Identificação das necessidades tecnológicas

1	Os profissionais técnicos alocados deverão exercer os serviços de: <ul style="list-style-type: none"> Monitoramento preventivo – que tem por objetivo garantir que os serviços finalísticos estejam em pleno funcionamento e livre de gargalos que prejudiquem a performance adequada. Monitoramento proativo – que tem por objetivo averiguar, constantemente, eventuais falhas de segurança, final de vida útil de equipamentos, estimativas de esgotamento de infraestrutura por aumento de uso e demanda. Melhoramentos – que tem por objetivo adequar configurações, arquiteturas, processos, métodos, sistemas e outros com o objetivo de auferir melhor segurança, disponibilidade e performance. Correções – que tem por objetivo identificar causas de problemas, diagnosticando-os e corrigindo-os de forma a reestabelecer serviços na qualidade, segurança e performance estabelecidos. Incluem-se os serviços de melhoria para evitar que tais problemas ocorram novamente. Provisionamento de informações – que tem por objetivo a extração de informações e elaboração de relatórios e documentos que demonstrem dados sobre a utilização, segurança, qualidade e performance do ambiente.
2	Os profissionais técnicos devem ser capazes de operar as seguintes tecnologias: <ul style="list-style-type: none"> Servidores físicos – instalação, monitoramento, configuração, instalação de software, aplicação de patches de segurança, verificação de performance, cluster de servidores. Servidores virtuais – instalação, monitoramento, configuração, instalação de software, aplicação de patches de segurança, verificação de performance, criação de máquinas virtuais, redes virtuais, criação de scripts. Servidores de aplicações instalação, monitoramento, configuração, instalação de software, aplicação de patches de segurança, verificação de performance, criação sítios. Storage - instalação, monitoramento, configuração, instalação de software, aplicação de patches de segurança, verificação de performance, configuração de máquinas virtuais, clonagem; criação de áreas de dados; criação de scripts; migração de dados; rotinas de backup e restauração; importação e exportação de dados; segmentação de dados; reorganização de espaço lógico e físico; monitoramento de saúde de discos e de controladoras. Servidores de banco de dados - instalação, monitoramento, configuração, instalação de software, aplicação de patches de segurança, verificação de performance, configuração de máquinas virtuais, clonagem; criação de áreas de dados; criação de scripts; migração de dados; rotinas de backup e restauração; importação e exportação de dados; criação de tabelas, relacionamentos, índices, restrições, usuários; análise de performance; aplicação de patches de segurança; Firewall – instalação, monitoramento, configuração, implantação de regras, análise de logs, detecção de vulnerabilidades, VPNs. IPS/IDS – controle e segurança, proteção contra intrusão de rede, detecção e bloqueio de ameaças. Solução de Backup – backup, recuperação de desastres e gerenciamento de dados em infraestruturas virtuais e físicas. Rede física – instalação, gerência e configuração de switches; cabeamento estruturado, cabos UTP e fibras. Containerização de aplicações – instalação, monitoramento, configuração e atualização de aplicações em ambientes de contêineres; cluster que executam aplicativos em contêineres.

1.3. Demais requisitos necessários e suficientes à escolha da solução de TIC

1	Os serviços deverão ser mensurados por resultados, que contemple, entre outros: <ol style="list-style-type: none"> a fixação dos procedimentos e dos critérios de mensuração dos serviços prestados, abrangendo métricas, indicadores, valores aceitáveis etc.; a quantificação ou a estimativa prévia do volume de serviços demandados, para fins de comparação e controle; a definição de metodologia de avaliação da adequação dos serviços às especificações, com vistas a aceitação e pagamento; a utilização de um instrumento de controle, geralmente consolidado no documento denominado “ordem de serviço” ou “solicitação de serviço”; a definição dos procedimentos de acompanhamento e fiscalização a serem realizados concomitantemente à execução para evitar distorções na aplicação dos critérios. (Acórdão TCU nº 1453/2009 – Plenário).
2	Requisitos de capacitação: <ol style="list-style-type: none"> Para o pleno exercício das funções técnicas, os profissionais da contratada passarão por capacitação arquitetural do ambiente do ITI, onde serão repassadas informações sobre o ciclo de atividades operacionais, cuja contratada exercerá monitoramento e manutenção ininterruptos. A capacitação poderá ser realizada à distância ou presencialmente, a critério do ITI. Esta capacitação será realizada uma única vez, onde caberá à contratada garantir a absorção de conhecimentos necessários ao trabalho diário, bem como a transferência para os demais (ou novos) profissionais da contratada que virem a atuar na contratação. O evento de capacitação poderá ser fracionado em etapas ou assuntos, conforme planejamento do ITI. O ITI proverá o material didático e o ambiente tecnológico para a capacitação, que será realizada por profissionais do ITI que atualmente realizam as atividades objeto deste TR.
3	Requisitos de Manutenção: <ol style="list-style-type: none"> À contratada caberá exercer continuamente os processos de manutenção preventiva sempre que forem observadas possibilidades de melhoria, como aplicação de patches de segurança, atualização de software, configuração de regras de segurança, e outros. As atividades deverão passar por análise e aprovação prévia em ambiente de teste e/ou homologação antes de aplicação definitiva em ambiente de produção. À contratada caberá exercer, sempre que necessário ou demandado, as atividades de manutenção corretiva, evolutiva e adaptativa. Estas atividades estarão formalizadas por Ordens de Serviço, onde serão verificados o cumprimento de níveis de serviços constante neste TR.
4	Requisitos Legais: <ol style="list-style-type: none"> Lei Federal nº 8.666/1993: institui normas gerais para licitações e contratos na Administração Pública e dá outras providências; OU Lei nº 10.520, de 17 de julho de 2002 institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns. Decreto nº 10.024, de 20 de setembro de 2019 regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal. Decreto nº 7.174, de 12 de maio de 2010 Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União. Instrução Normativa SGD/ME nº 31, de 23 de março de 2021 Altera a Instrução Normativa nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de

	<p>soluções de Tecnologia da Informação e Comunicação TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação SISF do Poder Executivo Federal.</p> <p>f) Instrução Normativa SGD/ME nº 202, de 18 de setembro de 2019 altera a Instrução Normativa nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação SISF do Poder Executivo Federal.</p> <p>g) Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação SISF do Poder Executivo Federal.</p> <p>h) Instrução Normativa SEGES/ME nº 73, de 5 de agosto de 2020 dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.</p> <p>i) Instrução Normativa SEGES/MP nº 1, de 10 de janeiro de 2019 dispõe sobre Plano Anual de Contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações no âmbito da Administração Pública federal direta, autárquica e fundacional e sobre o Sistema de Planejamento e Gerenciamento de Contratações.</p> <p>j) Instrução Normativa SEGES/MP nº 3, de 26 de abril de 2018 Estabelece regras de funcionamento do Sistema de Cadastro Unificado de Fornecedores – Sicaf, no âmbito do Poder Executivo Federal.</p> <p>k) Instrução Normativa SEGES/MP nº 5, de 26 de maio de 2017 dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.</p> <p>l) Portaria STI/MP nº 4, de 6 de março de 2017 dispõe sobre recomendações técnicas para mensuração de software ou de resultados de serviços de desenvolvimento, manutenção e sustentação de software no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação SISF.</p> <p>m) Portaria STI/MP nº 20, de 14 de junho 2016 dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional.</p> <p>n) Decreto nº 9.178, de 23 de outubro de 2017 regulamenta o art. 3º da Lei nº 8.666, de 21 de junho de 1993, para estabelecer critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal direta, autárquica e fundacional e pelas empresas estatais dependentes, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública – CISAP;</p> <p>o) Decreto nº 7.903, de 4 de fevereiro de 2013 estabelece a aplicação de margem de preferência em licitações realizadas no âmbito da administração pública federal para aquisição de equipamentos de tecnologia da informação e comunicação que menciona;</p> <p>p) Decreto nº 9.507, de 21 de setembro de 2018 dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;</p> <p>q) Portaria SGD/ME nº 6.432, de 15 de junho de 2021 Estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação SISF do Poder Executivo Federal.</p> <p>r) Portaria SGD/ME nº 4.668, de 23 de maio de 2022 – Altera o Anexo II da Portaria SGD/ME nº 6.432, de 15 de junho de 2021.</p> <p>s) Modelo de contratação de serviços de operação de infraestrutura e de atendimento de usuários de TIC do SISF/ME que detalha, conforme Portaria supracitada, as práticas e orientações a serem aplicadas em serviços de operação de infraestrutura e atendimento a usuários de TIC.</p> <p>t) Parecer no 1/2021/CNS/CGU/AGU - que recomenda aos agentes da administração pública federal encarregados de realizar contratações públicas, que, no exercício de suas atribuições funcionais, consultem o Guia Nacional de Contratações Sustentáveis do ITI.</p> <p>u) Guia Nacional de Contratações Sustentáveis, Câmara Nacional de Sustentabilidade – CNS, DE-COR/CGU/AGU, agosto/2021, 4a edição.</p>
5	<p>Requisitos de Manutenção:</p> <p>a) À contratada caberá exercer continuamente os processos de manutenção preventiva sempre que forem observadas possibilidades de melhoria, como aplicação de patches de segurança, atualização de software, configuração de regras de segurança, e outros. As atividades deverão passar por análise e aprovação prévia em ambiente de teste e/ou homologação antes de aplicação definitiva em ambiente de produção.</p> <p>b) À contratada caberá exercer, sempre que necessário ou demandado, as atividades de manutenção corretiva, evolutiva e adaptativa.</p> <p>c) Estas atividades estarão formalizadas por Ordens de Serviço, onde serão verificados o cumprimento de níveis de serviços constante neste TR.</p>
6	<p>Requisitos Temporais:</p> <p>a) Os serviços serão demandados mensalmente, com periodicidade fixa mensal. Caso a OS venha a ser aberta em dia que não seja o primeiro dia do mês, ela terá validade até o último dia do mesmo mês, sendo faturado proporcionalmente ao número de dias do mês.</p> <p>b) Mesmo havendo flutuação dos números de dias de cada mês, o contrato será faturado em parcelas de igual valor, descontados eventuais glosas e sansões.</p>
7	<p>Requisitos de Segurança e Privacidade:</p> <p>a) No que couber, o “Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade” deverá ser observado (vide Seção 7 do Anexo da IN SGD/ME nº 1/2019. Guia disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSiparaContratacoesdeTI.pdf).</p> <p>b) De acordo com os capítulos 5 e 8 da Declaração de Práticas de Certificação de Autoridade Certificadora Raiz da ICP-Brasil, disponível em http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf.</p> <p>c) De acordo com a Política de Segurança da ICP-Brasil, disponível em https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais/Resolucao193_DOCICP02.pdf.</p>
8	<p>Requisitos Sociais, Ambientais e Culturais:</p> <p>Para os eventuais serviços presenciais, o profissional da contratada deverá usar vestuário compatível e identificação por crachá da empresa, além de portar documentação de identificação civil, obrigatórios para o ambiente de Centro de Dados.</p>
9	<p>Requisitos de Projeto e de Implementação:</p> <p>Por esta contratação tratar-se de monitoramento e manutenção de estrutura já implantada, os eventuais projetos e implantações de novos serviços que ocorrerem durante a vigência contratual serão tratados futuramente.</p>
10	<p>Requisitos de Implantação:</p> <p>Para o início dos serviços, a contratada deverá constituir o Plano de Implantação, que será um compilado dos seguintes instrumentos:</p> <p>a) Plano de Trabalho Operacional - Define as rotinas básicas de trabalho, conforme detalhado na seção "Requisitos de Metodologia de Trabalho";</p> <p>b) Plano de Comunicação - Define as pessoas e formas de contato, tanto para procedimentos diários quanto para comunicação emergencial. O plano de comunicação deve incluir o mecanismo e ferramenta para gestão de chamados de TIC.</p> <p>c) Ferramentas de Operação e Gestão - definem as ferramentas que serão utilizadas para gestão, como para abertura de chamados, base de conhecimento, monitoramento (NOC e SOC) e outros. O documento deve explicitar o nome da ferramenta, o site do fabricante, os requisitos de hardware e software, entre outros. A escolha e a instalação das ferramentas (no ambiente do ITI) será definido pelo ITI durante a reunião inicial do contrato.</p> <p>d) Política de Segurança da Informação (POSIN) - da contratada, que definem as respectivas políticas de segurança, conforme detalhado na seção "Requisitos de Segurança da Informação".</p> <p>e) Termo de Sigilo e de proteção de dados pessoais – da contratada, adequado a Lei Geral de proteção de dados pessoais (13.709/2018), que defina a manutenção do sigilo, as condutas, responsabilidades e sanções diante do conhecimento, ciência, manipulação, posse de dados ou informações sensíveis, tanto ao negócio quanto pessoais.</p> <p>O Plano de Implantação deve ser capaz de responder aos seguintes questionamentos:</p> <p>a) Quem é o preposto da contratada, seu substituto e as formas de contato?</p> <p>b) Qual é o canal da empresa para comunicação emergencial?</p> <p>c) Quais são os canais para abertura e gestão de chamados? (mais de um obrigatoriamente)</p> <p>d) Quem são os profissionais da contratada alocados no contrato? Qual é a formação de cada um e as competências segundo o catálogo de serviços do ITI?</p> <p>e) Esses profissionais foram aprovados quanto à comprovação de experiência descritos na seção "Perfis profissionais" do Anexo - Catálogo de Serviços de TIC para Assinaturas Avançadas do ITI, neste TR?</p> <p>f) Quais ferramentas fazem parte da operação e da gestão do contrato? Onde elas estão instaladas?</p> <p>g) Quais são os prepostos e as outras empresas relacionadas ao serviço deste TR, onde deverá eventualmente haver interação mútua?</p> <p>h) Quais acessos serão criados para o monitoramento remoto? Quais controles sobre credenciais de acesso serão criados?</p> <p>i) Quais profissionais serão autorizados a adentrar fisicamente, eventualmente e quando estritamente necessário, na Sala Cofre?</p> <p>j) Quais são as rotinas de manutenção periódica e testes e quanto elas serão realizadas?</p>
11	<p>Requisitos de Garantia e Manutenção:</p> <p>a) Todos os serviços prestados pela contratada deverão possuir no mínimo um ano de garantia. Para tal gestão, serão utilizadas Ordens de Serviço, abertura de chamados e outros registro formais de demandas.</p> <p>b) A contratada se responsabiliza por quaisquer defeitos e vícios referentes aos serviços prestados, mesmo que o prazo de garantia se estenda à vigência do contrato.</p>
12	<p>Requisitos de Metodologia de Trabalho:</p> <p>A contratada deverá apresentar o Plano de Trabalho Operacional contemplando integralmente os requisitos e normativos a seguir. Este plano deverá ser ajustado a critério do</p>

	<p>ITI sempre que solicitado. Ainda, o plano passará por revisão semestral de avaliação e ajustes.</p> <p>A prestação de serviços contratada deve estar alinhada com os seguintes instrumentos que compõem o Plano de Trabalho Operacional:</p> <p>a) Modelo de contratação de serviços de operação de infraestrutura e de atendimento de usuários de TIC do SISP/ME, disponível no endereço https://www.gov.br/governodigital/pt-br/contratacoes/modelo-de-contratacao-de-servicos-de-operacao-de-infraestrutura-e-de-atendimento-a-usuarios-de-tic e com a Portaria SGD/ME no 6.432, de 15 de junho de 2021, disponível em https://www.gov.br/governodigital/pt-br/contratacoes/portaria-sgd-me-no-6-432-de-15-de-junho-de-2021; cujos valores financeiros presentes no Anexo II foram alterados pela Portaria SGD/ME no 4.668, de 23 de maio de 2022, disponível em https://www.in.gov.br/en/web/dou/-/portaria-sgd-me-n-4-668-de-23-de-maio-de-2022-402107009.</p> <p>b) Compilado de documentos que formam o Doc-ICP, disponível em https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais;</p> <p>c) Norma ABNT NBR ISO/IEC 20.000 - é uma norma de sistema de gestão de serviços (SGS). Ela especifica os requisitos para o provedor de serviço planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGS;</p> <p>d) Norma ABNT NBR ISO/IEC 20.001 - esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização;</p> <p>e) Norma ABNTNBR ISO IEC 27.002 – Código de Prática para Gestão da Segurança da Informação;</p> <p>f) Norma ABNTNBR ISO IEC 27.005 - Gestão de Riscos de Segurança da Informação;</p> <p>g) Norma ABNTNBR ISO IEC 27.007 - Diretrizes para Auditoria de Sistemas de Gestão da Segurança da Informação;</p> <p>h) Norma ABNT NBR 11515 – Critérios de Segurança Física Relativos ao Armazenamento de Dados;</p> <p>i) NC nº 02-IN01-DSIC-GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações;</p> <p>j) NC nº 04-IN01-DSIC-GSIPR, Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC;</p> <p>k) NC nº 08-IN01-DSIC-GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais;</p> <p>l) NC nº 10-IN01-DSIC-GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a SIC, APF direta e indireta;</p> <p>m) NC nº 14-IN01-DSIC-GSIPR, estabelece princípios, diretrizes e responsabilidades relacionados à SIC para o tratamento da informação em ambiente de computação em nuvem;</p> <p>n) NC nº 19-IN01-DSIC-GSIPR, Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da APF, direta e indireta;</p> <p>o) Procedimentos operacionais e normativos internos do ITI;</p> <p>p) Demais normativos expedidos ou publicados pela Administração Pública Federal.</p>
	<p>O Plano de Trabalho Operacional deverá detalhar, no mínimo, o cronograma de execução mensal das atividades técnicas e operacionais relacionadas aos serviços detalhados no Anexo - Catálogo de Serviços de TIC para Assinaturas Avançadas do ITI. Este plano poderá ser alterado conforme necessidades do ITI.</p> <p>O Plano de Trabalho Operacional deverá conter, no mínimo, os elementos necessários para a realização dos seguintes processos de trabalho:</p> <p>a) Monitoramento periódico;</p> <p>b) Manutenções e rotinas operacionais pré-estabelecidas;</p> <p>c) Gerenciamento de requisição de serviços;</p> <p>d) Gerenciamento de mudanças;</p> <p>e) Gerenciamento de documentação e conhecimento;</p> <p>f) Gerenciamento de problemas; e</p> <p>g) Gerenciamento de riscos, vulnerabilidades, incidentes.</p>
13	<p>O modelo de execução do Plano de Trabalho Operacional deve adotar metodologias ágeis em projetos de infraestrutura a exemplo da aplicação do conceito de DevSecOps. Para tal, o plano deve detalhar o uso de ferramentas que gerenciem, controlem e/ou automatizem os seguintes componentes:</p> <p>a) Controle de versão;</p> <p>b) Integração contínua;</p> <p>c) Testes contínuos;</p> <p>d) Gerenciamento de configuração e deployment;</p> <p>e) Gerenciamento de vulnerabilidades;</p> <p>f) Gerenciamento de documentação;</p> <p>g) Monitoramento contínuo;</p> <p>h) Containerização;</p> <p>i) Orquestração e automatização;</p> <p>j) Segurança integrada; e</p> <p>k) Gerenciamento integrado de demandas integrada.</p>
14	<p>Requisitos de Segurança da Informação e Privacidade:</p> <p>No que couber, o “Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade” deverá ser observado (vide Seção 7 do Anexo da IN SGD/ME nº 1/2019. Guia disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSiparaContratacoesdeTI.pdf).</p> <p>A empresa contratada deverá possuir uma Política de Segurança da Informação (POSIN), ou equivalente, aderente ao disposto na IN GSI/PR nº 1, de 27 de maio de 2020, incluindo políticas ou normas para proteção de dados pessoais vigentes e atualizadas, com processo de revisão periódico formalizado e institucionalizado, de forma a garantir, dentre outros requisitos, o uso de sistemática e procedimentos de segurança da informação para assegurar não apenas a disponibilidade, a integridade, a confidencialidade e a autenticidade, mas também a consistência, a privacidade e a confiabilidade dos dados e informações tratados pela Solução de TIC.</p> <p>Esta POSIN deverá conter, obrigatoriamente e explicitamente, aspectos que:</p> <ul style="list-style-type: none"> • Propiciem a disponibilidade da solução de TIC contratada; • Evitem vazamento de dados e fraudes digitais; • Definam processos de gestão de segurança da informação que envolvam a solução de TIC; • Possibilitem a rastreabilidade de forma a manter trilha de auditoria de segurança da informação; • Assegure a continuidade do negócio implementado pela solução; • Realizem o tratamento de dados pessoais (Lei 13709/2018) e informações classificadas, conforme legislação vigente; • Prevejam a realização de auditoria de SIC (Segurança da Informação e Comunicação) de conformidade dos requisitos de segurança da informação previstos pela contratação; • Assegurem a gestão e tratamento de incidentes de forma sistematizada; e • Indiquem diretrizes para o desenvolvimento e obtenção de software seguro. <p>Deve-se observar na construção dos artefatos de planejamento da contratação, no que couber, as diretrizes constantes de Guias e frameworks de Segurança da Informação e Privacidade publicados pela SGD.</p> <ul style="list-style-type: none"> • A definição dos requisitos de segurança da informação deve considerar as três dimensões de ações: • Prevenção: a capacidade de prevenir a ocorrência de incidentes de segurança; • Detecção: a capacidade de prover uma resposta rápida na identificação daqueles incidentes de segurança que não puderam ser prevenidos; e • Correção: a capacidade em restaurar ou mitigar o impacto daqueles incidentes de segurança detectados. <p>Durante o período de ambientação, a contratada deverá realizar em conjunto com o ITI uma análise de impacto na privacidade dos dados pessoais relacionada à Solução de TIC, considerando o descrito pelo relatório de impacto à proteção de dados pessoais, conforme previsto na Lei nº 13.709/2018. Esta análise deverá ser atualizada quando da concepção de qualquer novo projeto, produto ou serviço.</p> <p>Durante a vigência contratual, após o período de ambientação, a contratada deverá realizar e apresentar mensalmente uma análise/avaliação de riscos da arquitetura de Solução de TIC, indicando os eventos de risco ao qual o sistema está exposto, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada pela contratante. Este relatório deverá ser anexo à entrega dos serviços mensais.</p> <p>Durante a vigência contratual, após o período de ambientação, a contratada deverá mapear, documentar, atualizar e apresentar mensalmente a documentação que descreve a arquitetura física e lógica da Solução de TIC. Este relatório deverá incluir a descrição dos controles de segurança da informação e privacidade implementados em cada componente descrito na arquitetura física e lógica.</p>

	<p>Durante a vigência contratual, após o período de ambientação, em sintonia com a Lei Geral de Proteção de Dados, a contratada deverá apresentar, no que for cabível, a Matriz de responsabilidades descrevendo a atribuição das responsabilidades pela segurança da informação na organização, pela privacidade (encarregado), identificação dos gestores de serviços com dados pessoais, operador(es) de tratamento de dados, relacionada ao objeto da contratação.</p> <p>Durante a vigência contratual, após o período de ambientação, a contratada deverá executar mensalmente análise de vulnerabilidades na Solução de TIC, para detecção de vulnerabilidades técnicas e execução de medidas para seu saneamento ou contenção.</p> <p>A POSIN da contratada deverá ser assinada pelo respectivo quadro societário ou seu representante legal.</p>
15	<p>Outros Requisitos Aplicáveis:</p> <p>A contrata deve ainda adequar-se aos seguintes componentes de gestão:</p> <ul style="list-style-type: none"> • Catálogo de Serviços de TIC para Assinaturas Avançadas do ITI, anexo deste TR. • Base de conhecimento (para padronização do atendimento, retenção do conhecimento e agilidade na execução dos serviços), que deverá ser implantada pela contratada no ambiente do ITI durante o período de ambientação contratual. <p>Ferramenta de Gerenciamento de Serviços de TIC (ITSM), fornecida pela contratada (sem custos adicionais ao ITI), que deverá ser implantada no ambiente do ITI durante o período de ambientação contratual. Esta ferramenta deverá, no mínimo, ser capaz de:</p> <ul style="list-style-type: none"> • gerenciar chamados técnicos, com registro de timestamp dos estados de abertura, fechamento e reabertura com fins de mensurar o tempo de atendimento de cada chamado; • gerenciar, de modo individualizado (apartado), os incidentes e as solicitações de mudanças; • implementar as diretrizes constantes dos processos formalizados de mudanças, incidentes e configuração; • implementar o fluxo de classificação de chamados conforme processos formalizados; • implementar controles temporais por categoria de chamado; • possibilitar a extração de dados analíticos e consolidados com vistas a permitir a verificação de níveis mínimos de serviço; • assegurar a integridade, autenticidade e disponibilidade dos dados processados e armazenados; e • possibilitar a aferição de satisfação do atendimento pelo demandante do serviço. <p>A Ferramenta de Gerenciamento de Serviços de TIC (ITSM) deverá permitir a aferição:</p> <ul style="list-style-type: none"> • do tempo total de atendimento do chamado; • do tempo que o chamado permaneceu em cada estado; • se determinado chamado foi ou não reaberto; • da quantidade total de chamados atendidos em determinado período; • da quantidade total de chamados atendidos dentro do prazo esperado, durante determinado período; e • da quantidade total de chamados reabertos, em determinado período. <p>Nos casos onde for possível a utilização de Automação Robótica de Processos (RPA), a documentação e operação desta tecnologia deverá contemplar, no mínimo:</p> <ul style="list-style-type: none"> • funcionalidades de low code para construção de scripts de automação; • integração com aplicativos corporativos; e • orquestração e administração, incluindo configuração, monitoramento e segurança. <p>Poderão ser utilizados, quando desejáveis para a boa gestão e sem custos para o ITI, Ferramentas de Monitoramento de Desempenho de Aplicações (APM) e Ferramentas de Monitoramento de Desempenho e Diagnóstico de Redes (NPM).</p> <p>Ferramentas para o Network Operations Center (NOC), utilizada pela contratada (sem custos adicionais ao ITI), que deverá ser implantada pela contratada no ambiente da contratada ou contratante, conforme classificação dos dados disponibilizados, durante o período de ambientação contratual, mantido, suportado e atualizado durante a vigência contratual. Estas ferramentas deverão, no mínimo, serem capazes de:</p> <ul style="list-style-type: none"> • gerenciar todos os ativos, hardware e software pertencentes ao escopo da solução (contemplando os três sítios da STI); • gerenciar a performance e disponibilidade destes ativos; • gerenciar os principais indicadores técnicos e pontos de eventual gargalo; • gerenciar e monitorar a qualidade e disponibilidade dos serviços prestados; • gerenciar e monitorar os erros de aplicação e identificar problemas de configuração e aplicação; • gerenciar e monitorar rotas, meios de comunicação e largura de banda; • gerenciar, acompanhar e auditar chamados e níveis de serviço (ITSM); • gerenciar e manter arquitetura e representação gráfica da infraestrutura física e lógica; • gerenciar e alertar manutenções preventivas e agendamento de eventos; • gerenciar e monitorar incidentes de redes e infraestruturas; e • integrar alertas e monitoramento com sistemas de gerenciamento de incidentes e vulnerabilidades do SOC. <p>Ferramentas e sistemas para o Security Operations Center (SOC), utilizados pela contratada (sem custos adicionais ao ITI), que deverão ser implantados pela contratada no ambiente disponibilizado pelo ITI durante o período de ambientação contratual, mantido, suportado e atualizado durante a vigência contratual. Estas ferramentas deverão, no mínimo, serem capazes de:</p> <ul style="list-style-type: none"> • monitorar sistemas da infraestrutura típica de SOC (hardware e software), como firewalls, antivírus, IPS/IDS, SIEM, SOAR, soluções de detecção de vulnerabilidades e incidentes, sistemas de controle de acesso físico e lógico, e outros; • identificar, classificar, tratar, mitigar ou transferir, manual ou por automação, riscos inerentes aos sistemas, bem como da infraestrutura e aplicações (SOAR); • gerenciar incidentes de segurança e vazamentos de informação e suas evidências; • gerenciar evidências de vulnerabilidades; • gerenciar ciclo de vida de eventos sistemas como syslog, bem como de evidências geradas por serviços, aplicações e sistemas; • gerenciar e versionar configuração e patches de atualização de ativos como servidores, switches, roteadores, appliances, sistemas operacionais, bancos de dados, aplicações e bibliotecas para fins de identificação, registro e controle das vulnerabilidades; • gerenciar dados de sistema de correlação de eventos e de informações de segurança e vulnerabilidade (SIEM); • adequar-se ao fluxo de plano de tratamento e resposta a incidente; • integrar com ferramentas de análise de vulnerabilidade e de teste de penetração (pentests); e • fornecer dados para trilhas de auditoria em segurança da informação. <p>A aprovação ou solicitação de substituição dos mecanismos supracitados caberá exclusivamente ao ITI.</p> <p>A contratada deve prover preferencialmente o uso de ferramentas livres na gestão e operação contratual. Quando da impossibilidade do uso de ferramenta livre para determinado tema, assunto ou tarefa, a contratada deverá exportar todos os dados de gestão, mensalmente, durante a vigência contratual e ao encerramento do contrato. O ITI avaliará a eventual aquisição de ferramenta, na hipótese de vantagem justificada e necessária, quando comparada com alternativas gratuitas e livres.</p>

1.4. Descrição da necessidade (justificativa para a contratação)

1.4.1. O Instituto Nacional de Tecnologia da Informação - ITI, autarquia federal criada pelo Art. 12 da Medida Provisória 2.200-2 de 24 de agosto de 2001, com sede e foro no Distrito Federal, vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz - AC Raiz da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil e, além disso, teve suas competências ampliadas pelo Decreto 10.543 de 13 de novembro de 2020.

1.4.2. Para dar cumprimento às suas competências, o ITI conta com órgãos específicos que compõem a sua estrutura organizacional. Dentre estes, cabe à Diretoria de Infraestrutura de Chaves Públicas - DINFRA, por meio da Coordenação-Geral de Infraestrutura e Segurança da Informação – CGISI, o planejamento, coordenação e execução dos

processos referentes à gestão da infraestrutura tecnológica e da segurança da informação e da Coordenação-Geral de Operações, o planejamento criptográfico e de aplicações para atendimento às necessidades finalísticas do Instituto.

1.4.3. Assim, a CGISI e CGOPE implementam um processo permanente de modernização, visando o aperfeiçoamento da sua infraestrutura tecnológica, dos recursos criptográficos e das aplicações. Deste modo, a melhoria contínua relacionada ao seu ambiente tecnológico e de aplicações para o atendimento às demandas, em especial às áreas fins, é fundamental. Com o Decreto 10.543 de 13 de novembro de 2020, o Instituto recebeu mais uma grande responsabilidade: prover toda a infraestrutura de Assinaturas Avançadas, que é ofertada por meio de serviços digitais dos mais diversos órgãos, tais como, INSS, Senatran, Juntas Comerciais entre outros. Vale ressaltar também que este serviço tem crescido de forma exponencial, auferindo um aumento de 18 vezes, comparando-se os cenários de março a setembro de 2021.

1.4.4. Nota-se que manter este ambiente de infraestrutura tecnológica, criptográfica e de aplicações disponível em regime ininterrupto tem demandando grande esforço por parte da equipe CGISI e CGOPE, visto que, a Autarquia não possui corpo próprio de servidores e os atuais contratos contendo trabalho terceirizado não suportam este tipo de atividade no regime mencionado.

1.4.5. Dessa forma, a CGSI e a CGOPE identificaram a necessidade de contratação de empresa para prestação de serviços técnicos continuados na área de tecnologia da informação e comunicação, com o objetivo de sustentar e operar os serviços de infraestrutura e aplicações relacionadas a assinatura avançada. Esta contratação elevará a qualidade dos serviços suportados e fornecidos aos órgãos da administração e sociedade, incorporando gerenciamento e monitoramento adequados à criticidade dos ambientes e suporte técnico.

2. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

2.1. Estrutura de TIC – Assinaturas Eletrônicas Avançadas do ITI:

2.1.1. O ITI realiza o serviço de assinaturas avançadas atualmente por meio dos seguintes equipamentos:

- Servidores físicos e servidores virtuais, plataformas em nuvem pública, plataformas de virtualização, plataformas de gerenciamento de infraestrutura em containers, servidores de aplicação, servidores web, servidores proxy, serviço de diretório, serviço de armazenamento e compartilhamento de arquivos, correio eletrônico, processos de DevOps;
- Storages, soluções de hiperconvergência, switches SAN, soluções de NAS, fitotecas (robôs de backup), sistema de armazenamento e backup centralizado, media servers; bancos de dados transacionais e analíticos e ferramentas de ETL;
- Switches, roteadores, ativos de redes WIFI, MCU e endpoints de videoconferência, central de telefonia e terminais VoIP, links de comunicação, cabeamento estruturado;
- Firewalls, IPS/IDS, Web Filter, WAF, antivírus, antispam, VPN, gerenciamento de certificados digitais;

2.1.2. Estes equipamentos estão instalados da seguinte forma:

- Servidores físicos configurados em cluster;
- Serviços e aplicações instalados em servidores virtualizados no cluster;
- Cluster de servidores virtuais para a solução de contêineres;
- Storage conectado ao cluster com redundância de múltiplos caminhos.

2.1.3. Os sistemas externos estão disponíveis nos sítios:

- <https://verificador.iti.gov.br/verifier-2.7/>
- <https://assinador.iti.br/>

2.1.4. Os serviços finalísticos oferecidos por essa estrutura são os seguintes:

- Assinatura eletrônica do tipo avançada – o portal realiza assinaturas avançadas em documentos .DOC ou .DOCX ou .ODT ou .PDF;
- Geração de chave eletrônica do tipo avançada – ao realizar a primeira assinatura no portal, é gerado automaticamente um certificado avançado para o usuário que possuir conta govbr prata ou ouro;
- Manutenção das chaves em ambiente seguro – o data center está localizado na sala cofre do ITI, atendendo aos requisitos de segurança nível 3;
- Replicação dos dados entre os sítios de redundância – serão disponibilizados 3 sítios: dois em Brasília e um em Florianópolis;
- Verificar a conformidade do padrão de assinatura digital da Infraestrutura de Chaves Públicas Brasileira – aferir se um arquivo assinado está em conformidade com o DOC-ICP-15;

2.1.5. Os serviços técnicos realizados são os seguintes:

- Gerenciamento de Serviços de TIC;
- Sustentação de Aplicações;
- Armazenamento e Backup;
- Sustentação de Banco de Dados;
- Administração de Dados;
- Conectividade e Comunicação;
- Segurança de TIC;
- Monitoramento de Serviços de TI;

2.1.6. Os indicadores de produtividade atuais são:

- Número de assinaturas realizadas por mês: média de 700.000.
- Número de chaves mantidas: 756.489 no dia 15/03/2022.
- Número de chaves criadas por mês: média de 100.000.

2.1.7. Os perfis técnicos atualmente utilizados para manter os serviços são os seguintes (Qtd/Perfil):

Gerenciamento de Serviços e de Segurança de TIC:

- (Um) Gerente de infraestrutura de tecnologia da informação;
- (Um) Gerente de segurança da informação;

Infraestrutura (Sustentação de Infraestrutura para Aplicações, Armazenamento e Backup, Sustentação de Banco de Dados, Administração de Dados, Conectividade e Comunicação, Monitoramento de Serviços de TIC, Apoio técnico):

- (Um) Analista de sistemas de automação Pleno;
- (Dois) Administrador de sistemas operacionais Pleno;
- (Dois) Analista de suporte computacional Pleno;
- (Dois) Analista de suporte computacional Júnior;
- (Um) Administrador de banco de dados Pleno;
- (Um) Analista de redes e de comunicação de dados Pleno;

Segurança de TIC.

- (Dois) Administrador em segurança da informação Pleno;
- (Um) Administrador em segurança da informação Sênior;

Obs1: A descrição das competências profissionais dos perfis supracitados encontra-se na tabela da seção 11.44 da Portaria SGE/ME No 6.432/2021.

Obs2: Os números acima não determinam o quantitativo mínimo de pessoas da equipe que a contratada deverá utilizar no provimento dos serviços contratados; e serve tão somente para a estimativa de competências profissionais e esforço humano atualmente necessários para realizar o monitoramento e manutenção do ambiente. Enquanto o os profissionais da contratada não estarão em regime de dedicação exclusiva e podem ser compartilhados em outras necessidades da contratada, exige-se que a disponibilidade dos serviços contratados atue em regime ininterrupto (24x7), todos os dias, inclusive feriados, durante toda a vigência contratual.

2.1.8. As competências laborais da equipe envolvem:

- Controle de versão;
- Integração contínua;
- Testes contínuos;
- Gerenciamento de configuração e deployment;
- Monitoramento contínuo;
- Containerização;
- Orquestração;
- Segurança integrada; e
- Gerenciamento integrado de demandas integrada.

3. ANÁLISE DE SOLUÇÕES

3.1. IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	Prover os serviços de operação de infraestrutura, com a utilização de servidores do quadro de pessoal do ITI.
2	Prover os serviços de operação de infraestrutura, por meio da requisição de empregados e servidores públicos requisitados de empresas e órgãos públicos para atuação junto ao ITI.
3	Contratar serviços especializados de operação de infraestrutura por meio de processo licitatório.

3.2. ANÁLISE COMPARATIVA DE SOLUÇÕES

Requisito			
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?			
Solução	Sim	Não	Não se Aplica
Solução 1	X		
Solução 2	X		
Solução 3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)			
Solução	Sim	Não	Não se Aplica
Solução 1			X
Solução 2			X
Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)			
Solução	Sim	Não	Não se Aplica
Solução 1			X
Solução 2			X
Solução 3			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?			
Solução	Sim	Não	Não se Aplica
Solução 1			X
Solução 2			X
Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)			
Solução	Sim	Não	Não se Aplica
Solução 1			X
Solução 2			X
Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)			
Solução	Sim	Não	Não se Aplica
Solução 1			X
Solução 2			X
Solução 3			X

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

4.1. **Solução 1** (Prover os serviços de operação de infraestrutura, com a utilização de servidores do quadro de pessoal do ITI) – Inviável, pois o ITI não possui servidores capacitados e em número suficiente para suprir a demanda pelos serviços de sustentação do ambiente. Ainda, com o crescimento que o serviço vem demonstrando, será necessária a ampliação do ambiente e dos serviços de manutenção relacionados.

4.2. **Solução 2** (Prover os serviços de operação de infraestrutura, por meio da requisição de empregados e servidores públicos requisitados de empresas e órgãos públicos para atuação junto ao ITI) – Inviável, pelo fato de o ITI não possuir orçamento específico para a alocação de profissionais públicos suficientes para os serviços necessários. Quanto aos servidores públicos de outros órgãos, não é uma prática comum da APF, visto a escassez de profissionais, especialmente os de TIC, nos órgãos públicos.

5. **ANÁLISE COMPARATIVA DE CUSTOS (TCO)**

5.1. **CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE**

Solução Viável 3 - Contratar serviços especializados de atendimento e sustentação por meio de processo licitatório.
Custo Total de Propriedade – Memória de Cálculo
O Custo Total de Propriedade é uma métrica de análise que tem como objetivo calcular os custos de vida e de aquisição de um produto, ativo ou sistema. Levando-se em consideração que este estudo trata da contratação de serviços de TI, que não há análises do tipo “comprar x fazer”, este item não é aplicável.

5.2. **MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)**

Estimativa de TCO ao longo dos anos

Descrição da solução	Estimativa de TCO ao longo dos anos				Total
	Ano 1	Ano 2	Ano 3	Ano 4	
Solução Viável 3	R\$2.985.683,54	R\$2.985.683,54	R\$2.985.683,54	R\$2.985.683,54	R\$11.942.734,15

Obs: os valores acima não apresentam eventuais reajustes contratuais.

6. **DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA**

6.1. Contratação de empresa especializada para o fornecimento Solução de ampliação da maturidade de ambiente computacional envolvendo a implantação e operação de Central de Suporte Técnico, com registro e acompanhamento de serviços especializados, visando prover ao ITI, serviços de manutenção e evolução da saúde operacional com processos de trabalho aferidos e remunerados exclusivamente por Itens de Configuração (parcelas fixas mensais), e ajustados por Níveis de Serviço.

6.2. **Bens e serviços que compõem a solução**

ITEM	Descrição do Bem ou Serviço	Código CATSER	Unidade de Medida	Quantidade estimada
1	GERENCIAMENTO	27014	Unidade mensal	24
2	INFRAESTRUTURA	27014	Unidade mensal	24
3	SEGURANÇA	27014	Unidade mensal	24

7. **ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO**

Item	NATUREZA	EXERCÍCIO	QUANTIDADE ANUAL DEMANDADA	ANUAL ESTIMADO
1	CUSTEIO - 33904011 - Suporte de Infraestrutura de TIC	2022 em diante	12 meses por ciclo contratual	R\$ 2.985.683,54
Valor total estimado para o contrato:				R\$ 5.971.367,08

8. **DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO**

8.1. O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pelos integrantes TÉCNICO e REQUISITANTE em harmonia com o disposto no art. 11 da Instrução Normativa nº 31/2021/SGD/ME, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE DA CONTRATAÇÃO – uma vez considerados os seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade. Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que RECOMENDAMOS O prosseguimento da pretensão.

8.2. O serviço de Assinaturas Avançadas foi criado pelo ITI e institucionalizado por meio do Decreto no 10.543 de 13 de novembro de 2020 e pela Lei No 14.063 de 23 de setembro de 2020.

8.3. O ambiente computacional para manter tais serviços são fornecidos pelo ITI em uma arquitetura de tríplice clusterização. A manutenção desse ambiente é atualmente feita por servidores do ITI, profissionais terceirizados e por profissionais da UFSC.

8.4. Nos últimos doze meses, este ambiente teve um crescimento exponencial de cerca de 10x o número de assinaturas inicialmente estimado. Com o crescimento da utilização do serviço torna-se essencial aumentar o grau de qualidade dos serviços técnicos de monitoramento e de manutenção da solução.

8.5. Visto a limitação de servidores técnicos capacitados do ITI, é imperativo a realização de contração de empresa especializada no provimento de serviços de operação de infraestrutura para o este ambiente computacional.

8.6. Este estudo visa analisar e propor a melhor alternativa técnica e econômica para o ITI.

9. **APROVAÇÃO E ASSINATURA**

9.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria ITI nº 59, publicada no BS no 46/2021, de 27 de outubro de 2021.

9.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO

Marcelo Fenoll Ramal

SIAPE: 1776363

INTEGRANTE REQUISITANTE

José Rodrigues Gonçalves Junior

SIAPE 2094611

AUTORIDADE MÁXIMA DA ÁREA DE TIC

(OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)

APROVO, o Estudo Técnico Preliminar tendo em vista que o presente planejamento está em conformidade com os requisitos administrativos necessários ao cumprimento do objeto. Não atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos em são administráveis e a área requisitante priorizará o fornecimento de todos os elementos ora relacionados necessários à consecução dos benefícios pretendidos, pelo que recomenda a contratação proposta.

Felipe Bimbato Rodrigues

Coordenador de Tecnologia da Informação e Comunicações - COTIC

Matrícula/SIAPE: 1820968



Documento assinado eletronicamente por **Marcelo Fenoll Ramal**, **Fiscal de Contrato - Técnico**, em 09/06/2022, às 11:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Jose Rodrigues Gonçalves**, **Coordenador-Geral**, em 09/06/2022, às 14:41, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).
Nº de Série do Certificado: 22608



Documento assinado eletronicamente por **Felipe Bimbato Rodrigues**, **Coordenador**, em 13/06/2022, às 15:17, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).
Nº de Série do Certificado: 22850



A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0555636** e o código CRC **9FBF78E3**.