

# Estudo Técnico Preliminar - 6/2022

## 1. Informações Básicas

Número do processo: 00100.003688/2021-94

## 2. Objeto

### **Operação de Infraestrutura de TIC (Sítio Avançada)**

Contratação 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).

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.

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.

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.

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.

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.

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.

### **3. Descrição da necessidade**

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.

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.

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.

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.

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.

#### 4. Área requisitante

Área Requisitante	Responsável
Coordenador-Geral de Infraestrutura e Segurança da Informação	José Rodrigues Gonçalves Júnior

#### 5. Necessidades de Negócio

1.1	<b>Identificação das necessidades de negócio</b>
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"> <li>• PR – Localizado no anexo do Palácio do Planalto, Brasília, DF;</li> <li>• UFSC – Localizado em Florianópolis/SC.</li> </ul> O acesso físico eventual se dará exclusivamente no sítio localizado em Brasília/DF.
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 <a href="https://www.gov.br/governodigital/pt-br/contratacoes/modelo-de-contratacao-de-servicos-de-operacao-de-infraestrutura-e-de-atendimento-a-usuarios-de-tic">https://www.gov.br/governodigital/pt-br/contratacoes/modelo-de-contratacao-de-servicos-de-operacao-de-infraestrutura-e-de-atendimento-a-usuarios-de-tic</a> . e com a Portaria SGD/ME no 6.432, de 15 de junho de 2021, disponível em <a href="https://www.gov.br/governodigital/pt-br/contratacoes/portaria-sgd-me-no-6-432-de-15-de-junho-de-2021">https://www.gov.br/governodigital/pt-br/contratacoes/portaria-sgd-me-no-6-432-de-15-de-junho-de-2021</a> .
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.

## 6. Necessidades Tecnológicas

Identificação das necessidades tecnológicas	
1	<p>Os profissionais técnicos alocados deverão exercer os serviços de:</p> <ul style="list-style-type: none"> <li>• Monitoramento preventivo – que tem por objetivo garantir que os serviços finalísticos estejam em pleno funcionamento e livre de gargalos que prejudiquem a performance adequada.</li> <li>• 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.</li> <li>• Melhoramentos – que tem por objetivo adequar configurações, arquiteturas, processos, métodos, sistemas e outros com o objetivo de auferir melhor segurança, disponibilidade e performance.</li> </ul>

	<ul style="list-style-type: none"> <li>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.</li> <li>Provimento 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.</li> </ul>
2	<p>Os profissionais técnicos devem ser capazes de operar as seguintes tecnologias:</p> <ul style="list-style-type: none"> <li>Servidores físicos – instalação, monitoramento, configuração, instalação de software, aplicação de patches de segurança, verificação de performance, cluster de servidores.</li> <li>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.</li> <li>Servidores de aplicações instalação, monitoramento, configuração, instalação de software, aplicação de patches de segurança, verificação de performance, criação sítios.</li> <li>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 restauro; importação e exportação de dados; segmentação de dados; reorganização de espaço lógico e físico; monitoramento de saúde de discos e de controladoras.</li> <li>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 restauro; importação e exportação de dados; criação de tabelas, relacionamentos, índices, restrições, usuários; análise de performance; aplicação de patches de segurança;</li> <li>Firewall – instalação, monitoramento, configuração, implantação de regras, análise de logs, detecção de vulnerabilidades, VPNs.</li> <li>IPS/IDS – controle e segurança, proteção contra intrusão de rede, detecção e bloqueio de ameaças.</li> <li>Solução de Backup – backup, recuperação de desastres e gerenciamento de dados em infraestruturas virtuais e físicas.</li> <li>Rede física – instalação, gerência e configuração de switches; cabeamento estruturado, cabos UTP e fibras.</li> <li>Containerização de aplicações – instalação, monitoramento, configuração e atualização de aplicações em ambientes de contêineres; cluster que executem aplicativos em contêineres.</li> </ul>

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

### Demais requisitos necessários e suficientes à escolha da solução de TIC

1	<p>Os serviços deverão ser mensurados por resultados, que contemple, entre outros:</p> <p>a) a fixação dos procedimentos e dos critérios de mensuração dos serviços prestados, abrangendo métricas, indicadores, valores aceitáveis etc.;</p> <p>b) a quantificação ou a estimativa prévia do volume de serviços demandados, para fins de comparação e controle;</p> <p>c) a definição de metodologia de avaliação da adequação dos serviços às especificações, com vistas a aceitação e pagamento;</p> <p>d) a utilização de um instrumento de controle, geralmente consolidado no documento denominado “ordem de serviço” ou “solicitação de serviço”;</p> <p>e) 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).</p>
2	<p>Requisitos de capacitação:</p> <p>a) 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.</p> <p>b) 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</p>

	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	<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>
4	<p>Requisitos Legais:</p> <p>a) Lei Federal nº 8.666/1993: institui normas gerais para licitações e contratos na Administração Pública e dá outras providências; OU</p> <p>b) 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.</p> <p>c) 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.</p> <p>d) 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.</p> <p>e) 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 soluções de Tecnologia da Informação e Comunicação TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação SISP 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 SISP 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 SISP 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 Cadastramento 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 SISP.</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</p>

	<p>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 SISP 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 SISP/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: <a href="https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf">https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf</a>).</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 <a href="http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf">http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf</a>.</p> <p>c) De acordo com a Política de Segurança da ICP-Brasil, disponível em <a href="https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais/Resolucao193_DOCICP02.pdf">https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais/Resolucao193_DOCICP02.pdf</a>.</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>
	<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</p>

10	<p>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 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 <a href="https://www.gov.br/governodigital/pt-br/contratacoes/modelo-de-contratacao-de-servicos-de-operacao-de-infraestrutura-e-de-atendimento-a-usuarios-de-tic">https://www.gov.br/governodigital/pt-br/contratacoes/modelo-de-contratacao-de-servicos-de-operacao-de-infraestrutura-e-de-atendimento-a-usuarios-de-tic</a> e com a Portaria SGD/ME no 6.432, de 15 de junho de 2021, disponível em <a href="https://www.gov.br/governodigital/pt-br/contratacoes/portaria-sgd-me-no-6-432-de-15-de-junho-de-2021">https://www.gov.br/governodigital/pt-br/contratacoes/portaria-sgd-me-no-6-432-de-15-de-junho-de-2021</a>; cujos valores financeiros presentes no Anexo II foram alterados pela Portaria SGD/ME no 4.668, de 23 de maio de 2022, disponível em <a href="https://www.in.gov.br/en/web/dou/-/portaria-sgd/me-n-4.668-de-23-de-maio-de-2022-402107009">https://www.in.gov.br/en/web/dou/-/portaria-sgd/me-n-4.668-de-23-de-maio-de-2022-402107009</a>.</p> <p>b) Compilado de documentos que formam o Doc-ICP, disponível em <a href="https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais">https://www.gov.br/iti/pt-br/assuntos/legislacao/documentos-principais</a>;</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>
13	<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> <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>
	<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: <a href="https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf">https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf</a>).</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</p>

14	<p>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"> <li>• Propiciem a disponibilidade da solução de TIC contratada;</li> <li>• Evitem vazamento de dados e fraudes digitais;</li> <li>• Definam processos de gestão de riscos de segurança da informação que envolvam a solução de TIC;</li> <li>• Possibilitem a rastreabilidade de forma a manter trilha de auditoria de segurança da informação;</li> <li>• Assegure a continuidade do negócio implementado pela solução;</li> <li>• Realizem o tratamento de dados pessoais (Lei 13709/2018) e informações classificadas, conforme legislação vigente;</li> <li>• Prevejam a realização de auditoria de SIC (Segurança da Informação e Comunicação) de conformidade dos requisitos de segurança da informação previstos pela contratação;</li> <li>• Assegurem a gestão e tratamento de incidentes de forma sistematizada; e</li> <li>• Indiquem diretrizes para o desenvolvimento e obtenção de software seguro.</li> </ul> <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"> <li>• A definição dos requisitos de segurança da informação deve considerar as três dimensões de ações:</li> <li>• Prevenção: a capacidade de prevenir a ocorrências de incidentes de segurança;</li> <li>• Detecção: a capacidade de prover uma resposta rápida na identificação daqueles incidentes de segurança que não puderam ser prevenidos; e</li> <li>• Correção: a capacidade em restaurar ou mitigar o impacto daqueles incidentes de segurança detectados.</li> </ul> <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> <p>Outros Requisitos Aplicáveis:</p> <p>A contrata deve ainda adequar-se aos seguintes componentes de gestão:</p> <ul style="list-style-type: none"> <li>• Catálogo de Serviços de TIC para Assinaturas Avançadas do ITI, anexo deste TR.</li> <li>• 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.</li> </ul> <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>
----	--

- 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.

A Ferramenta de Gerenciamento de Serviços de TIC (ITSM) deverá permitir a aferição:

- 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.

Nos casos onde for possível a utilização de Automação Robótica de Processos (RPA), a documentação e operação desta tecnologia deverá contemplar, no mínimo:

- funcionalidades de low code para construção de scripts de automação;
- integração com aplicativos corporativos; e
- orquestração e administração, incluindo configuração, monitoramento e segurança.

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 (NPMD).

- 15 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:

- 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.

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:

- 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.

A aprovação ou solicitação de substituição dos mecanismos supracitados caberá exclusivamente ao ITI.

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.

## 8. Estimativa da demanda - quantidade de bens e serviços

Estrutura de TIC – Assinaturas Eletrônicas Avançadas do ITI:

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;

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

Os sistemas externos estão disponíveis nos sítios:

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

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;

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;

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

Os perfis técnicos atualmente estimados para manter os serviços são os seguintes:

- 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.

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.

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

## 9. JUSTIFICATIVA PARA A CONTRATAÇÃO

### Contextualização e Justificativa da Contratação

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.

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.

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.

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.

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.

## 10. Levantamento de 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.

## 11. 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

## 12. Registro de soluções consideradas inviáveis

**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.

**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.

## 13. Análise comparativa de custos (TCO)

**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.

#### 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	<b>R\$11.942.734,15</b>

Obs: os valores acima não apresentam eventuais reajustes contratuais.

#### 14. Descrição da solução de TIC a ser contratada

### ANEXO - CATÁLOGO DE SERVIÇOS DE TIC PARA ASSINATURAS AVANÇADAS DO ITI

#### Categoria de serviços

Este anexo apresenta as principais atividades relacionadas ao serviço contrato, mas não limita a atuação da empresa nas competências e ações necessárias para a efetiva atuação.

A operação de infraestrutura de serviços de TIC abrange serviços continuados para monitoramento e sustentação do ambiente computacional que podem ser subdivididos nas seguintes categorias:

#### Gerência de serviços de TIC:

- Implantar e manter os processos de Gerenciamento de Serviços de TIC definidos pelo ITI, baseado nas melhores práticas, utilizando ferramenta (s) especializada(s);
- Implantar os recursos tecnológicos para o NOC e o SOC;
- Operar, manter, atualizar e criar fluxos de processos na ferramenta de Gerenciamento de Serviços de TIC;
- Adaptar os fluxos básicos de incidentes, requisição, mudanças, problemas e configuração, com o desenho de formulários e criação de regras e validações;

- Criar e adaptar outros fluxos de trabalho, ancorados nos processos básicos de gerenciamento de serviços de TI, o que inclui desenho de formulários e criação de regras e validações;
- Discutir os requisitos dos fluxos de trabalho, para propor a sua adequação às boas práticas de GSTI;
- Identificar melhorias nos processos básicos de gerenciamento de serviços de TIC sob a ótica das melhores práticas de GSTI preconizadas pelo ITIL;
- Utilizar os indicadores chave de desempenho para apoiar a atividade de evolução dos processos;
- Difundir o conhecimento de melhores práticas para as equipes de TIC;
- Realizar as integrações das ferramentas necessárias para o correto funcionamento dos processos;
- Resolver falhas relativas aos fluxos e à ferramenta de suporte ao gerenciamento de serviços de TIC;
- Elaborar, manter e atualizar os relatórios de acompanhamento dos processos e indicadores de níveis de serviço;
- Elaborar relatórios gerenciais e técnicos quando solicitados;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Manter os processos de gerenciamento de incidente, catálogo de serviços, configuração e ativo de serviço, problema, mudança, conhecimento, disponibilidade e níveis de serviço (cabe ao ITI a decisão final sobre implantação ou modificação de processos no âmbito do escopo da contratação);
- Realizar a interface de comunicação entre as demais categorias de serviços e a contratante.

### **Suporte computacional**

- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe a camada de sustentação de serviços e aplicações do ITI;
- Operar, administrar e manter os servidores físicos e virtuais do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados à camada de sustentação de serviços e aplicações do ITI;
- Realizar configurações, alterações e otimizações no ambiente de sustentação de serviços e aplicações do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente.

### **Armazenamento e Backup**

- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de backup e armazenamento do ITI;
- Executar, manter, atualizar, implantar e apoiar na criação das políticas de backup do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de backup e armazenamento do ITI;
- Realizar configurações, alterações e otimizações no ambiente de backup e armazenamento do ITI;
- Realizar testes de restore com definição de frequência a critério do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente.

### **Sustentação de Banco de Dados**

- Projetar, instalar, implantar, operar, administrar e manter o conjunto de ferramentas, softwares e hardwares que compõe recursos e soluções relacionadas a bancos de dados do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de banco de dados do ITI;
- Realizar configurações, alterações e otimizações no ambiente de banco de dados do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Registrar chamados para fornecedores das soluções;
- Elaborar e manter atualizada a documentação de todo o ambiente.

### **Administração de Dados**

- Apoiar na auditoria, análise, revisão de documentação relativas à modelagem de dados;
- Construção de queries;
- Apoiar na manutenção de repositório de metadados;
- Manter esquemas de banco de dados;
- Elaborar e manter modelo de dados;
- Apoio na Elaboração e definição de política de segurança do Banco de Dados;
- Realizar apuração Especial;
- Confecção e manutenção de documentação e de procedimentos técnicos;

- Validação de modelos de dados quanto às melhores práticas de modelagem;
- Desenvolvimento, execução, teste e documentação de rotinas de ETL;
- Instalar, configurar, otimizar, parametrizar ferramenta ETL;
- Sugerir automatização das rotinas.

### **Redes e comunicação de dados**

- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de conectividade e comunicação do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de conectividade e comunicação do ITI;
- Realizar configurações, alterações e otimizações no ambiente de conectividade e comunicação do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente.

### **Segurança de TIC**

- Implantar ambiente de SOC para monitoramento da STI objeto deste contrato.
- Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõe o ambiente de segurança de TIC do ITI;
- Tratar incidentes, problemas, requisições e mudanças relacionados ao ambiente de segurança de TIC do ITI;
- Realizar configurações, alterações e otimizações no ambiente de segurança de TIC do ITI;
- Realizar testes de vulnerabilidades dos sistemas e serviços de TIC do ITI, identificando os riscos e sugerindo ações para o devido tratamento;
- Apoiar na elaboração e manutenção da política de segurança do ITI;
- Apoiar na elaboração e manutenção do plano de continuidade de negócio do ITI;
- Apoiar na elaboração e manutenção do plano de gerenciamento de risco do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Configurar, monitorar, operar e gerenciar equipamentos relacionados ao ambiente de SOC, como firewall, IPS, e outros;
- Atuar na detecção de falhas e brechas;

- Prover respostas rápidas a eventuais ataques;
- Realizar testes de penetração (Pentest);
- Elaborar e manter atualizada a documentação de todo o ambiente.

### **Monitoramento de Serviços de TIC**

- Implantar ambiente de NOC para monitoramento da STI objeto deste contrato.
- Realizar o monitoramento dos sistemas, aplicações, serviços e infraestrutura de TIC do ITI através de ferramenta(as) especializada(s);
- Executar o plano de comunicação realizando os acionamentos dos responsáveis pela resolução dos incidentes, bem como manter informadas as partes interessadas;
- Operar, administrar e manter o conjunto de ferramentas e softwares que compõe a solução de monitoramento de TIC do ITI;
- Realizar configurações, alterações e otimizações na solução de monitoramento de TIC do ITI;
- Manter o ambiente atualizado observando as orientações previstas no gerenciamento de mudanças;
- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de toda a solução;
- Outros requisitos complementares estão descritos na seção "**Monitoração de Ambiente Tecnológico (NOC e SOC)**" deste anexo.

### **Atividades complementares / Apoio Técnico**

- Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, caso necessário;
- Elaborar e manter atualizada a documentação de todo o ambiente;
- Identificar, mapear e atualizar o inventário de ativos de TIC;
- Apoiar e acompanhar os processos de gerenciamento de incidente, catálogo de serviços, configuração e ativo de serviço, problema, mudança, conhecimento, disponibilidade e níveis de serviço;
- Apoiar a elaboração de manuais e procedimentos operacionais;
- Apoiar a elaboração de boas práticas e da base de conhecimento.

### **Macro atividades por domínio**

**Ativos de Rede** - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; e Atualização.

**Servidores** - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; e Atualização.

**Aplicações** - Instalação (*deploy*); Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; e Atualização.

**Banco de dados** - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; Atualização; Criação de área de dados; Remoção de dados; Migração de dados; Execução de scripts; e Alteração de privilégios.

**Backup** - Execução de rotinas; Restauração; Checagem de backups; Simulação; e Atualização.

**Armazenamento e Storage** - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; Atualização; Criação de área de dados; Remoção de dados; Migração de dados; Execução de scripts; e Alteração de privilégios.

**Segurança da informação** - Instalação; Configuração; Manutenção preventiva; Manutenção corretiva; Otimização de performance; Investigação de falha; Investigação de incidente; Atualização; e Adequação de regras.

**Documentação** - Manutenção Procedimentos operacionais; testes e simulações; relatórios estatísticos; relatórios de falhas; relatórios de incidentes; relatórios investigativos; notas técnicas; e desenhos arquiteturais de TIC.

## **Tecnologias de Domínio**

Ambiente de armazenamento e rede de dados SAN - Storage Area Network (Rede de Armazenamento de Dados), utilizando fibre channel, ethernet e iscsi, composta por software e hardware de armazenamento de dados suportando minimamente um total de 200 (duzentos) Terabytes e solução de backup (Tape Library) com tecnologia LTO-4 ou superior e capacidade mínima de 100 fitas;

Redes físicas e endereçamento IP – planejamento, atualização, criação, desenho, implantação, administração e manutenção de redes e serviços TCP/IP – incluindo implementações em IPV4 e IPV6 que comprove minimamente o envolvimento dos seguintes componentes, serviços e soluções: Desenho de infraestrutura para redes IPV4 e IPV6, configuração de endereçamentos para alcance global, otimização de entrega de pacotes com formato de cabeçalho simplificado, IPSec nativo, comunicação fim a

fim, VPN site to site, multipath, loadbalancing, autonomous system com load sharing, bloco de endereçamento próprio, roteamento entre redes físicas e virtuais (VLAN's), implementação de IPSec para redes IPV4 e IPV6 em plataformas Unix-like (OpenBSD, FreeBSD) e Linux, configuração de serviço de DNS, DHCP e escopos DHCP6, IPV6 em dupla pilha, configuração de switches core considerando o uso de IPV6;

Plataforma de computação em nuvem privada, administração, orquestração e configuração de containers kubernetes e docker através de ferramentas (HELM, RANCHER, OPENSIFT e semelhantes);

Sistemas de proxy, balanceamento de carga e filtro de conteúdo (WAF);

Soluções de segurança da informação para proteção de rede e de host (Antivirus, Firewall, HIDS/IDS/IPS, SIEM e SOAR);

Solução de armazenamento em massa, consolidada e de forma centralizada como DELL Unity, VMAX, Powervault ou semelhantes;

Solução para monitoramento de ativos de redes, links de rede e servidores corporativos, recursos, serviços e aplicações, por meio de instalação e configuração de clientes ou agentes para plataformas Unix-like (OpenBSD, FreeBSD), Linux e Windows, incluindo a configuração de alertas de forma integrada com escalonamento por e-mail, be/ou SMS com a disponibilização de painéis, mapas ou dashboards de monitoramento para visualização do estado atual do ambiente e problemas.

Plataforma de sistemas operacionais e bancos de dados para servidores corporativos, suportando e executando ao menos as plataformas de sistemas operacionais e de bancos de dados abaixo:

- Plataformas de Sistemas Operacionais:
  - Ubuntu – versões 18, 20 ou superior;
  - FreeBSD – versão 11, 12 ou superior;
  - OpenBSD – versão 6, 7 ou superior;
  - CentOS 7 ou superior;
  - Microsoft Windows Server – versões 2019 ou superior;
  - RedHat Linux – versões 6, 7 ou superior;
- Plataformas de Bancos de Dados:
  - MySQL (MariaDB);
  - PostgreSQL;
  - MongoDB;
  - Elastic;
  - Redis;
  - Microsoft SQL Server.



Solução de gerenciamento, orquestração e provisionamento automático de máquinas virtuais e físicas, implementada e gerenciada pelas soluções de código aberto (Open Source) e Vmware;

Solução de provisionamento automatizado de servidores físicos e virtuais, bem como, de contêineres em Docker e kubernetes, utilizando sistemas operacionais nas plataformas Microsoft Windows, Debian, Ubuntu, RedHat, CentOS, e Unix-like (OpenBSD e FreeBSD), integrando ainda, ambientes de armazenamento de dados que tenha capacidade de suportar storage;

Solução de gerenciamento de containers e aplicações, utilizando ferramentas de Desenvolvimento Contínuo e Integrados (CI/CD) com GITLAB ou GITHUB;

Ferramentas de ITSM (OTRS, ZUNNY, REDMINE ou similar) para abertura automática e automação de chamados através de integrações;

Soluções de gestão e registro de eventos de sistema como Graylog, Prometheus, Nagios (ou Zabbix e similares), instalação, configuração, operação e integração, para ambiente composto por pelo menos 100 (cem) servidores virtualizados, no mínimo 8 hosts principais e integração de plataformas de virtualização VMWare ESXi;

Solução de backup utilizando robôs Tandberg NEOxl 40 (ou similares) e suítes de backup Veeam, Bacula (ou similares);

Soluções em shell scripting e operação de sistemas operacionais através de terminais, e em automatização de configuração e orquestração de infraestrutura utilizando Ansible, Puppet, Chef ou solução similar.

## Perfis profissionais

Os perfis profissionais que atuarão nas diferentes categorias são padronizados com vistas a possibilitar publicação periódica de pesquisa salarial pela SGD.

Cada perfil profissional possui uma característica e um propósito de atuação, conforme descrito a seguir:

Cod. CBO de Referência	PERFIL PROFISSIONAL DE REFERÊNCIA	DESCRIÇÃO DA ATUAÇÃO
42124-20		

	<p><b>Analista de suporte computacional Júnior e Pleno</b></p>	<p>Profissional associado ao centro de dados. Presta serviços de gerenciamento físico e lógico de equipamentos, servidores, storages, entre outros equipamentos do centro de dados ou no ambiente virtualizado. Atua também no gerenciamento de backups, configuração de procedimentos de recuperação de desastres computacionais, gerenciamento de recursos computacionais avançados (a exemplo de Servidores de arquivos, de impressão, de comunicação institucional) que demandam alocação, configuração ou instalação de softwares ou construção e execução de scripts para o controle, monitoramento e gerenciamento desses recursos.</p> <p>Experiência mínima de dois anos para o perfil Pleno e de um ano para o perfil Júnior nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI <b>OU</b> caso o profissional apresente <u>ao menos duas</u> das certificações a seguir: a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation v3 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) HDI SCTL - Support Center Team Lead (ou superior); g) ITIL® intermediário SOA - Service Offerings and Agreements; h) Veritas Certified Specialist (VCS) Netbackup; i) Veeam Certified Engineer (VMCE); j) Veeam Certified Architect (VMCA).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos quatro</u> das certificações indicadas.</p>

51425-5, 1425-15	<b>Gerente de infraestrutura de tecnologia da informação</b>	<p>Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais alocados no monitoramento, controle e operação da infraestrutura de TIC, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de infraestrutura de TIC, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de operações na infraestrutura de TIC.</p> <p>Experiência mínima de três anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente <u>ao menos duas</u> das certificações a seguir: a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation v3 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Certificação da Extreme Networks ECS Data CenterVDX; g) Cisco Certified Network Professional (CCNP); h) Cisco Certified Networking Associate (CCNA); i) Cisco Certified Network Professional (CCNP); j) Huawei Certified ICT Associate (HCIA); k) Extreme Networks ECS Data Center VDX.</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos quatro</u> das certificações indicadas.</p>
62123-5	<b>Administrador de banco de dados Pleno</b>	<p>Profissional responsável pela administração, operação, gerenciamento, carga de dados, otimização e monitoramento dos recursos de banco de dados. Presta serviços de gerenciamento dos esquemas de banco de dados, alocação e</p>

		<p>administração de recursos físicos e lógicos, realiza dimensionamentos e prospecções de uso, monitora incidentes e promove adequações, aprimoramentos e expansão dos recursos. Pode atuar na análise de dados propondo padrões e assegurando a normalização e melhor uso dos recursos para armazenamento e utilização de dados corporativos.</p> <p>Experiência mínima de dois anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.</p> <p>A experiência mínima poderá ser de apenas 50% do solicitado caso o profissional apresente certificação oficial de DBA nas tecnologias: a) Oracle (OCP ou OCA); ou b) Postgree.</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos uma</u> das certificações indicadas.</p>
72123-15	<b>Administrador de sistemas operacionais Pleno</b>	<p>Profissional que atua na camada de virtualização e orquestração de sistemas operacionais de servidores de dados. Presta serviços de configuração, instalação e ampliação de ambientes de containers. Responsável pela adequada operação, desempenho e uso racional de recursos utilizados pelos softwares básicos, orquestradores de containers e virtualizadores.</p> <p>Experiência mínima de dois anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades. A experiência mínima poderá ser de apenas um ano caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p>

		<p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente ao menos três das certificações a seguir: a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation v3 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Certificação da Extreme Networks ECS Data Center VDX; g) Cisco Certified Network Professional (CCNP); h) Cisco Certified Networking Associate (CCNA); i) Cisco Certified Network Professional (CCNP); j) Huawei Certified ICT Associate (HCIA); k) Extreme Networks ECS Data Center VDX; l) Certificação Certified Linux Administrator (LPIC-1 ou LPIC-2); m) Certificação Red Hat Certified System Administrator (RHCSA); n) Certificação Linux Enterprise Mixed Environment (LPIC-3); o) Certificação Red Hat Certified Engineer (RHCE).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos cinco</u> das certificações indicadas.</p>
82124-10, 2123-10	<b>Analista de redes e de comunicação de dados Pleno</b>	<p>Profissional que atua na intercomunicação de redes locais e de longa distância, com ou sem fio, assegurando a operação, desempenho e qualidade dos serviços de rede e comunicação de dados, bem como no aprimoramento e funcionamento adequados dos ativos de redes. Presta serviços de execução, aprimoramento e manutenção dos projetos de redes, além da configuração e otimização de recursos de interconexão de dados.</p> <p>Experiência mínima de dois anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades. A experiência mínima poderá ser de apenas um ano caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p>

		<p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente ao menos três das certificações a seguir: a) HDI SCTL - Support Center Team Lead (ou superior); b) ITIL® intermediário SOA - Service Offerings and Agreements; c) ITIL Foundation v3 ou superior; d) ITIL® intermediário – Operational Support and Analysis Capability (OSA); e) ITIL® intermediário – Planning, Protection and Optimization (PPO); f) Certificação da Extreme Networks ECS Data Center VDX; g) Cisco Certified Network Professional (CCNP); h) Cisco Certified Networking Associate (CCNA); i) Cisco Certified Network Professional (CCNP); j) Huawei Certified ICT Associate (HCIA); k) Extreme Networks ECS Data Center VDX; l) Certificação Certified Linux Administrator (LPIC-1 ou LPIC-2); m) Certificação Red Hat Certified System Administrator (RHCSA); n) Certificação Linux Enterprise Mixed Environment (LPIC-3); o) Certificação Red Hat Certified Engineer (RHCE).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos cinco</u> das certificações indicadas.</p>
102124-15, 2124-25	<b>Analista de sistemas de automação Pleno</b>	<p>Profissional responsável por assegurar utilização adequada de soluções de integração (CI) ou de entrega contínua (CD). Pode atuar como arquiteto de soluções e propor, projetar, executar e aprimorar arquiteturas de soluções necessárias à manutenção e melhoria das operações na infraestrutura de TIC. Pode atuar também como arquiteto de computação em nuvem, ou ainda como arquiteto de soluções híbridas.</p> <p>Experiência mínima de dois anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades. A experiência mínima poderá ser de apenas um ano caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p>

		<p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente ao menos duas das certificações a seguir: a) ferramentas de automação robótica de processos (RPA); b) Certified Kubernetes Administrator (CKA); c) Certified Kubernetes Security Specialist (CKS); d) Red Hat Certified Specialist in Containers and Kubernetes; e) Red Hat Certified System Administrator (RHCSA); f) Red Hat Certified Engineer (RHCE). A experiência mínima poderá ser de apenas um ano caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos quatro</u> das certificações indicadas.</p>
122123-20	<b>Administrador em segurança da informação Pleno e Sênior</b>	<p>Profissional responsável por assegurar a prestação de serviços de segurança da informação, incluindo o monitoramento e tratamento de incidentes, ações preventivas, implantação e monitoramento de controles de segurança, realização dos diferentes testes e inspeções de segurança. presta serviços e controle de segurança preventivo e reativo relacionado aos diferentes ativos da infraestrutura, bem como apoia na implementação das ações técnicas previstas na política de segurança.</p> <p>Experiência mínima de quatro anos nos serviços supracitados para o perfil Sênior e de dois anos para o perfil Pleno, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades. A experiência mínima poderá ser de 50% do solicitado caso o profissional tenha atuado em operações de Centro de Dados (CCD) na Presidência da República ou no ITI.</p> <p>A experiência mínima poderá ser de apenas 50% do solicitado caso o profissional apresente certificação oficial ou curso de</p>

		<p>graduação/especialização (acima de 80h/aula) em Segurança da Informação <b>OU</b> caso o profissional apresente <u>ao menos três</u> das certificações a seguir: a) Certificação Check Point Certified Security Expert (CCSE); b) Certified Information Security Manager (CISM); c) Systems Security Certified Practitioner (SSCP); d) Certified Information Systems Security Professional (CISSP); e) CompTIA Advanced Security Practitioner (CASP+); f) GIAC Security Expert (GSE).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos cinco</u> das certificações indicadas.</p>
131425-25	<b>Gerente de segurança da informação</b>	<p>Profissional com responsabilidade de coordenar e gerenciar a atuação dos demais profissionais de segurança da informação, garantindo a adequada prestação dos serviços, bem como controlando e planejamento operacionalmente as ações dessa equipe. Presta também apoio à tomada de decisão do órgão auxiliando na prospecção de soluções de segurança da informação, fornecimento de informações táticas e operacionais, e proposição de ações de aprimoramento dos serviços de segurança da informação seja preventiva ou reativa.</p> <p>Experiência mínima de três anos nos serviços supracitados, comprovada por meio de registro em Carteira de Trabalho ou contrato(s) executado(s) pelo funcionário, além da devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.</p> <p>A experiência mínima poderá ser de 50% do solicitado caso o profissional apresente certificação oficial ou curso de graduação /especialização (acima de 80h/aula) em Segurança da Informação <b>OU</b> caso o profissional apresente ao menos três das certificações a seguir: a) Certificação Check Point Certified Security Expert (CCSE); b) Certified Information Security Manager (CISM); c) Systems Security Certified Practitioner</p>



		<p>(SSCP); d) Certified Information Systems Security Professional (CISSP); e) CompTIA Advanced Security Practitioner (CASP+); f) GIAC Security Expert (GSE).</p> <p>Formação em curso superior completo na área de Tecnologia da Informação, ou qualquer formação de nível superior com pós-graduação na área de Tecnologia da Informação, com diploma, devidamente registrado, de conclusão de curso de graduação na área de Tecnologia da Informação ou nível superior em qualquer área com pós-graduação na área de Tecnologia da Informação em nível de especialização ou superior, fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação – MEC.</p> <p>A ausência da formação acadêmica supracitada poderá ser compensada por profissional que apresente <u>ao menos quatro</u> das certificações indicadas.</p>
n/a	<b>Preposto</b>	<p>O Preposto e seu substituto serão os responsáveis administrativos, com poderes de representante legal para tratar de todos os assuntos relacionados ao contrato, atuando à luz da Instrução Normativa nº 01/2019 da SGD/ME e suas revisões, e em atenção ao art. 68 da Lei nº. 8.666/93. Será atribuição sua gerir a execução do serviço, objeto do contrato, por parte da contratada, objetivando garantir a execução e entrega dos serviços dentro dos prazos estabelecidos e atendendo todos os requisitos especificados neste Termo de Referência; Gerir as solicitações de mudanças feitas pelo ITI, formalmente encaminhadas; Responder, perante o ITI, pela execução das solicitações; Participar periodicamente, a critério do ITI, de reuniões de acompanhamento das atividades referentes à prestação do serviço em execução. Não há obrigatoriedade do preposto disponível fisicamente nas dependências do ITI. Todavia, o preposto, obrigatoriamente, deverá estar disponível fisicamente nas dependências do ITI, quando solicitado, principalmente enquanto houver a execução da prestação de serviços por parte da contratada ao ITI.</p> <p>Experiência mínima de um ano nos serviços supracitados.</p> <p>Formação segundo grau completo.</p>

**Observação 1:** Cada Perfil profissional está associado a um ou mais CBO (Códigos Brasileiro de Ocupação) com vistas a estabelecer uma referência mais acurada a bases salariais de governo.

**Observação 2:** Caso a empresa opte por alocar parte da equipe dentro das instalações do ITI/PR, será cedido mobiliário completo e equipamentos de TIC para até três postos de trabalho. Neste caso, a permanência do profissional não configurará dedicação exclusiva de mão de obra.

Além das competências individuais supracitadas, específicas do cargo, a equipe deverá possuir as seguintes competências de atuação transversal: Controle de versão; Integração contínua; Testes contínuos; Gerenciamento de configuração e deployment; Monitoramento contínuo; Containerização; Orquestração; Segurança integrada; e Gerenciamento integrado de demandas integrada.

Todos os prestadores deverão ser registrados pelo regime CLT ou possuir contratos de prestação de serviços junto à contratada.

### **Monitoração de Ambiente Tecnológico (NOC e SOC)**

O serviço de monitoração do ambiente tecnológico deverá contemplar todos os elementos de hardware e software necessários a disponibilização dos serviços de TIC descritos neste TR e anexos.

Deverá também monitorar as instalações (*facilities*) de centro de dados e salas técnicas, quando houver disponível ferramenta adequada a esta monitoração.

Para a realização do monitoramento da infraestrutura de rede de dados e componentes de segurança da informação, a contratada deverá utilizar as ferramentas já implantadas no ambiente do ITI, ou sugerir novas quando as atuais se demonstrarem insuficientes para a gestão adequada. No caso de eventuais custos extras (licenciamento, implantação, configuração, adaptação, customização, migração, administração, etc), estes serão de inteira responsabilidade da contratada.

O serviço de Monitoração dos Serviços é responsável pela análise dos ativos, aplicações e serviços de TI do ITI em regime integral 24x7 (24 horas por dia, em 7 dias por semana), e deverá ser Remoto.

Os Serviços de TIC que serão objeto da avaliação de disponibilidade para efeito de mensuração de NMS deverão ser monitorados conforme determinação do ITI. Os demais ativos e serviços de TIC deverão ser monitorados a critério da contratada, sendo facultada à equipe técnica do ITI a solicitação de monitoração de itens específicos.

A equipe do NOC e SOC deverá ser capaz de tratar incidentes por meio de scripts ou procedimentos para reduzir o tempo de resolução dos mesmos.

A equipe do NOC e SOC deverá ser capaz de escalar para especialista de plantão, ou para outro que tenha maior capacidade técnica para resolução do incidente, de acordo com a necessidade específica do caso.

A contratada deverá implementar esquema de escalação de incidentes para analistas de maior conhecimento técnico, inclusive fora do horário de expediente, em regime 24x7.

Os serviços terão a disponibilidade mensurada conforme critérios estabelecidos pelo ITI.

No processo de gestão de incidentes, a equipe do NOC e SOC deverá tornar disponível as informações de detecção e tratamento de incidentes /problemas à respectiva equipe técnica responsável, para que esta tenha capacidade de responder o incidente/problema de forma mais célere.

A ferramenta de monitoração deverá ser configurada para automaticamente cadastrar incidentes na ferramenta de ITSM associados ao item/ativo adequado, a fim de permitir a tratativa e gestão dos incidentes.

A ferramenta de monitoração deverá ser capaz de prover dados para compor relatório específico de disponibilidade de Serviços de TIC ou de soluções de TIC.

Ao término do contrato, toda documentação e dados gerados pelas ferramentas deverão ser entregues ao ITI em modelo e padrões definidos por este.

## **Operação de Infraestrutura de TI.**

Este serviço assemelha-se ao terceiro nível de atendimento, onde especialistas da contratada realizam as diversas atividades técnicas preestabelecidas para manutenção periódica e atividades de reparo /restauração quando da ocorrência de incidentes e problemas.

O serviço de Operação de infraestrutura deverá ser capaz de projetar, planejar, implementar, administrar, operar e restabelecer serviços locais (*On-premises*) ou em cenário de infraestrutura híbrida nas diversas modalidades como: IaaS, PaaS e SaaS.

Os serviços de Operação de Infraestrutura deverão atuar no processo de tratamento de incidentes em regime de plantão 24x7, inclusive para incidentes específicos de segurança de TIC, que venham a ser reportados

no escopo de  
serviço de outros contratos do ITI, sem custo adicional.

Os serviços de Operação de Infraestrutura, quando necessário ou demandados por catálogo de serviços, deverão investigar incidentes e problemas a fim de identificar a causa raiz, propor e executar as correções necessárias, e também elaborar relatórios detalhados. Quando necessário deverá inclusive atuar em conjunto com outras contratadas do ITI, ou terceiros indicados e necessários.

Os serviços de Operação de Infraestrutura também compreenderão:

1. Solucionar ou viabilizar os diversos serviços da rede, analisando as ocorrências e diagnosticando os problemas, visando normalizar os procedimentos e cumprir os padrões de qualidade, prazo e prioridade estabelecidos;
2. Definir procedimentos de testes dos equipamentos e softwares implantados ou que sofrerão manutenção, antes de substituir os efetivos, visando manter controle dos impactos sobre as rotinas vigentes;
3. Definir e implementar configurações contra ataques de vírus de computador e invasão da rede local;
4. Auxiliar e propor mudanças nas definições dos requisitos de segurança, infraestrutura e tecnologia a serem utilizadas na implementação das soluções de TI;
5. Alimentar a base de conhecimento, com a descrição de solução de problemas resolvidos;
6. Configurar e administrar as redes LAN / MAN / WAN. Análise e correção de problemas em redes de transmissão de dados, diagnóstico e análise de desempenho das redes de dados;
7. Instalar e manter ativos de rede tais como switches e roteadores, em qualquer um dos sítios de prestação de serviço, conforme as políticas institucionais de segurança de informação;
8. Criar e remover rotas e redes locais virtuais (VLANs) a partir da configuração dos ativos de rede;
9. Fazer o contato e atuar na resolução de incidentes em conjunto com as empresas provedoras de enlaces de dados de longa distância;
10. Configurar e monitorar as implementações e aplicações que utilizam mecanismos de qualidade de serviço (QoS) e priorização de tráfego;
11. Atuar local ou remotamente nos ativos de rede para realizar configurações ou solucionar incidentes;
12. Elaborar a documentação de infraestrutura de rede, manuais para base de conhecimento e desenhos de topologia de rede;
13. Subsidiar os servidores da rede na elaboração de projetos de estruturas físicas e lógicas das redes;

14. Aplicar de forma proativa os patches para atualização de software e correção de falhas e vulnerabilidades nos ativos de rede;
15. Executar periodicamente testes de alta disponibilidade na infraestrutura da rede com o objetivo de validar o seu funcionamento;
16. Realizar configuração e operação dos ativos e recursos de rede dedicados à infraestrutura de armazenamento de dados e ao backup via rede;
17. Executar as rotinas de operação e administração do firewall, WAF, Proxy, GPO, visando garantir a disponibilidade, o melhor desempenho, a segurança e a continuidade da operação;
18. Administrar as soluções de detecção e prevenção de intrusões (IPS /IDS), incluindo configuração e testes de regras, filtragem de tráfego malicioso, resolução de problemas, atualização de regras, e outros, nas plataformas utilizadas pelo ITI;
19. Realizar suporte técnico por meio da administração, da análise, do diagnóstico e da solução de incidentes/problemas relacionados ao ambiente de virtualização (Hyper-v e VMware);
20. Realizar configuração, automatização e operação de ferramentas de "Operations Manager";
21. Administração, sustentação e suporte em máquinas virtuais virtualizadas envolvendo criação, clone, migração e crescimento horizontal;
22. Desenvolver templates de máquinas virtuais com os sistemas operacionais indicados pelo ITI;
23. Gerenciar cluster de virtualização com os recursos Físicos fornecidos pelo ITI;
24. Administrar e gerenciar servidores de aplicação/web;
25. Administrar, Operar e Suportar Banco de Dados;
26. Desenvolver Procedures, Querys, Scripts, Cargas de Dados em BD, Views, Triggers e Functions;
27. Modelar dados (Transacional e Multidimensional);
28. Construir mapas e processos de ETL. Apoiar à equipe de desenvolvimento de sistemas;
29. Recomendar as melhores práticas na área de Banco de Dados voltada para o negócio do ITI;
30. Utilizar ferramentas ETL de extração de dados, DW e Data Mining;
31. Acompanhar rotinas de backup por meio da ferramenta de monitoração para identificar possíveis erros;
32. Analisar logs de erros na ferramenta de backup para identificar melhor forma de correção;
33. Corrigir job's de backup por meio da ferramenta utilizada para restaurar o backup;

34. Desenhar e criar políticas de backup de acordo com a demanda do órgão, implementando as definições na ferramenta para atender os requisitos do ITI;
35. Restaurar dados de acordo com a demanda do ITI para recuperar informações perdidas;
36. Gerenciar armazenamento analisando o espaço utilizado por meio de relatórios para alertar sobre a disponibilidade de espaço;
37. Analisar o funcionamento do backup por meio de relatórios para apresentar e propor melhorias ao ITI;
38. Documentar e automatizar processos;
39. Realizar auditorias;
40. Emitir notas técnicas.

Os serviços abaixo representam as operações de Infraestrutura pré-determinados para outro ambiente do ITI, e que podem, em algum momento, fazerem parte do escopo das atividades periódicas da contratada:

1. Acompanhamento da manutenção do ambiente seguro (ongoing) - 52 vezes ao ano;
2. Tratamento dos registros de acesso - 52 vezes ao ano;
3. Backup do Sistema de CFTV (verificação) - 12 vezes ao ano;
4. Restauração de Backup do CFTV - 4 vezes ao ano;
5. Backup do Servidor Syslog (verificação) - 12 vezes ao ano;
6. Restauração de Backup do Syslog - 4 vezes ao ano;
7. Análise de registros de acesso aos Repositórios das Assinaturas Avançadas - 12 vezes ao ano;
8. Backup do Servidor de Arquivos (verificação) - 12 vezes ao ano;
9. Restauração de Backup do Servidor de Arquivos - 4 vezes ao ano;
10. Backup das bases de dados e arquivos de configuração (verificação) - 12 vezes ao ano;
11. Restauração de Backup da base de dados e arquivos de configuração - 4 vezes ao ano;
12. Backup do Sistema de Controle de Acesso (verificação) - 12 vezes ao ano;
13. Restauração de Backup do Sistema de Controle de Acesso - 4 vezes ao ano;
14. Backup do Sistema Antifraude (verificação) - 12 vezes ao ano;
15. Restauração de Backup do Sistema Antifraude - 4 vezes ao ano;
16. Análise da disponibilidade dos Repositórios das Assinaturas Avançadas - 12 vezes ao ano;
17. Atualização do SO dos Servidores - 4 vezes ao ano;
18. Backup do Servidor SFTP (verificação) - 12 vezes ao ano;
19. Restauração de Backup do Servidor SFTP - 4 vezes ao ano;
20. Revisão de acessos físicos - 4 vezes ao ano;

21. Revisão de acessos lógicos (servidores Intranet) - 4 vezes ao ano;
22. Revisão de acessos lógicos (servidores Internet) - 4 vezes ao ano;
23. Revisão de acessos lógicos (servidores offline) - 4 vezes ao ano;
24. Revisão de acessos lógicos (ativos de rede) - 2 vezes ao ano;
25. Revisão de acessos ao SIGAS - 4 vezes ao ano;
26. Revisão das topologias de rede e mapa de switches - 2 vezes ao ano;
27. Análises de vulnerabilidades - 12 vezes ao ano;
28. Teste do Plano de Continuidade de Negócio (PCN) - 2 vezes ao ano;
29. Encaminhar informações de disponibilidade/ indisponibilidade da infraestrutura das Assinaturas Avançadas para o setor de comunicação Social - 12 vezes ao ano;
30. Limpeza de logs dos scripts dos repositórios das Assinaturas Avançadas - 6 vezes ao ano;
31. Revisão dos documentos, termos e dossiês (Colaboradores, Vigilantes e Coordenadores) - 4 vezes ao ano;
32. Revisão das listas de profissionais (Site Principal (Brasília) e Site Contingência (Florianópolis/SC)) - 4 vezes ao ano;
33. Verificação dos hiperlinks e apontamentos no Site Web do ITI (Documentos principais e Repositórios) - 4 vezes ao ano;
34. Atualizar Formulário de Avaliação de Desempenho da Função - 1 vez ao ano;
35. Revisão das documentações (Manual de Administração do CCD) - 2 vezes ao ano;
36. Revisão das documentações (Análise e Avaliação de Risco) - 2 vezes ao ano;
37. Revisão das documentações (Análise de Risco de Firewall) - 2 vezes ao ano;
38. Revisão das documentações (Plano de Continuidade de Negócio) - 2 vezes ao ano;
39. Revisão das documentações (Manual Gestão de Pessoas) - 4 vezes ao ano;
40. Revisão das documentações (Matriz de Perfil de Acesso) - 2 vezes ao ano;
41. Revisão dos manuais de sistemas e tabela de equipamentos (Wiki) - 4 vezes ao ano.

Obs: durante a vigência contratual esta lista poderá ser ajustada tanto no quantitativo como na frequência, de acordo com necessidades do ITI.

## 15. Estimativa de custo total da contratação

Valor (R\$): 5.971.367,08

Resumo da Planilha Simplificada para Estimativa do Valor Mensal do Serviço				
ITEM	Categoria	Valor Mensal de Referência	Valor Anual de Referência	Valor Contratual de Referência
1	GERENCIAMENTO	R\$ 83.537,39	R\$ 1.002.448,66	R\$ 2.004.897,31
2	INFRAESTRUTURA	R\$ 101.843,27	R\$ 1.222.119,22	R\$ 2.444.238,44
3	SEGURANÇA	R\$ 63.426,31	R\$ 761.115,66	R\$ 1.522.231,32
TOTALIS		R\$ 248.806,96	R\$ 2.985.683,54	R\$ 5.971.367,08

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

## 16. Justificativa técnica da escolha da solução

Trata-se de única alternativa válida, segundo a Portaria SGD/ME no 6.432, de 15 de junho de 2021 (atualizada pela Portaria SGD/ME no 4.668/2022).



## 17. Justificativa econômica da escolha da solução

A estimativa de preços foi realizada com base na Portaria SGD/ME no 6.432/2021 (atualizada pela Portaria SGD/ME no 4.668/2022), onde em seu Art. 4º determina:

Art. 4º Para o planejamento da contratação e no momento da eventual prorrogação contratual, a definição do valor de referência e do valor máximo da contratação deverá utilizar como base a pesquisa salarial de preços e fator-k, previstos no Anexo II a esta Portaria.

§ 1º Os valores constantes no Anexo II, cumprem o disposto na Instrução Normativa Seges/ME nº 73, de 5 de agosto de 2020, para fins de pesquisa de preços das contratações que utilizarem os perfis e insumos do referido Anexo.

Ainda, conforme item 2 do Anexo II da portaria 4.668/2022, fica fixado o valor do fator-k da seguinte maneira:

2. O Fator-k a ser utilizado deve ser de **2,35**.

Para os cálculos abaixo utilizou-se como referência o valor de R\$ 6.000 para custos fixos técnicos anuais e R\$ 200 para custos fixos administrativos (ambos valores individuais).

Planilha Simplificada para Estimativa do Valor Mensal do Serviço					
ITEM	Categoria de Serviço			GERENCIAMENTO	
				Fator K:	2,35
	Perfil	Salário de referência (A)	Quantidade (B)	Custo unitário mensal do Perfil (C)	Custo total mensal por Perfil (D = C x B)
1	Gerente de infraestrutura de tecnologia da informação	R\$ 16.582,20	1	R\$ 38.968,17	R\$ 38.968,17
2	Gerente de segurança da informação	R\$ 18.369,88	1	R\$ 43.169,22	R\$ 43.169,22

<b>Quantitativo Total Equipe</b>	<b>2</b>	<b>Custo Total mensal (F)</b>	<b>R\$ 82.137,39</b>
--------------------------------------	----------	-----------------------------------	----------------------

Outros itens de custo para ITEM 1		
#	Descrição	Custo mensal (E)
1	Custos fixos técnicos (equipamentos, softwares, etc)	R\$1.000,00
2	Custos fixos administrativos (aluguel, energia, água, etc)	R\$400,00
	<b>Custo mensal Total Outros Itens (G)</b>	<b>R\$ 1.400,00</b>

<b>Valor Mensal de Referência do ITEM 1 (F+G)</b>	<b>R\$ 83.537,39</b>
---	----------------------

Planilha Simplificada para Estimativa do Valor Mensal do Serviço					
ITEM 2	Categoria de Serviço			INFRAESTRUTURA	
				Fator K:	2,35
	Perfil	Salário de referência (A)	Quantidade (B)	Custo unitário mensal do Perfil (C)	Custo total mensal por Perfil (D = C x B)
3	Analista de sistemas de automação - Pleno	R\$ 5.036,89	1	R\$ 11.836,69	R\$ 11.836,69
4	Administrador de sistemas operacionais Pleno	R\$ 4.787,76	2	R\$ 11.251,24	R\$ 22.502,47
5	Analista de suporte computacional Pleno	R\$ 4.475,40	2	R\$ 10.517,19	R\$ 21.034,38

6	Analista de suporte computacional Junior	R\$ 2.845,10	2	R\$ 6.685,99	R\$ 13.371,97
7	Administrador de banco de dados - Pleno	R\$ 6.506,01	1	R\$ 15.289,12	R\$ 15.289,12
8	Analista de redes e de comunicação de dados Pleno	R\$ 4.897,29	1	R\$ 11.508,63	R\$ 11.508,63
<b>Quantitativo Total Equipe</b>			<b>9</b>	<b>Custo Total mensal (F)</b>	<b>R\$ 95.543,27</b>

Outros itens de custo		
ITEM	Descrição	Custo mensal (E)
1	Custos fixos técnicos (equipamentos, softwares, etc)	R\$4.500,00
2	Custos fixos administrativos (aluguel, energia, água, etc)	R\$1.800,00
	<b>Custo mensal Total Outros Itens (G)</b>	<b>R\$ 6.300,00</b>

<b>Valor Mensal de Referência do ITEM 2 (F+G)</b>	<b>R\$ 101.843,27</b>
---	-----------------------

Planilha Simplificada para Estimativa do Valor Mensal do Serviço					
ITEM	Categoria de Serviço			SEGURANÇA	
				Fator K:	2,35
	Perfil	Salário de referência (A)	Quantidade (B)	Custo unitário mensal do Perfil (C)	Custo total mensal por Perfil (D = C x B)

9	Administrador em segurança da informação - Pleno	R\$ 7.257,31	2	R\$ 17.054,68	R\$ 34.109,36
10	Administrador em segurança da informação - Senior	R\$ 11.581,68	1	R\$ 27.216,95	R\$ 27.216,95
		<b>Quantitativo Total Equipe</b>	<b>3</b>	<b>Custo Total mensal (F)</b>	<b>R\$ 61.326,31</b>

Outros itens de custo		
ITEM	Descrição	Custo mensal (E)
1	Custos fixos técnicos (equipamentos, softwares, etc)	R\$1.500,00
2	Custos fixos administrativos (aluguel, energia, água, etc)	R\$600,00
	<b>Custo mensal Total Outros Itens (G)</b>	<b>R\$ 2.100,00</b>

<b>Valor Mensal de Referência do ITEM 3 (F+G)</b>	<b>R\$ 63.426,31</b>
---	----------------------

Resumo da Planilha Simplificada para Estimativa do Valor Mensal do Serviço				
ITEM	Categoria	Valor Mensal de Referência	Valor Anual de Referência	Valor Contratual de Referência
1	GERENCIAMENTO	R\$ 83.537,39	R\$ 1.002.448,66	R\$ 2.004.897,31
2	INFRAESTRUTURA	R\$ 101.843,27	R\$ 1.222.119,22	R\$ 2.444.238,44
3	SEGURANÇA	R\$ 63.426,31	R\$ 761.115,66	R\$ 1.522.231,32
<b>TOTAIS</b>		<b>R\$ 248.806,96</b>	<b>R\$ 2.985.683,54</b>	<b>R\$ 5.971.367,08</b>

Item.	Descrição do Bem ou Serviço	Quantidade	Unidade de medida	Valor unitário máximo	Valor total máximo
1	Gerenciamento	24	Val/mês	R\$ 83.537,39	R\$ 2.004.897,31
2	Infraestrutura	24	Val/mês	R\$ 101.843,27	R\$ 2.444.238,44
3	Segurança	24	Val/mês	R\$ 63.426,31	R\$ 1.522.231,32
			<b>Valor total estimado para o contrato:</b>		<b>R\$ 5.971.367,08</b>

Item	NATUREZA	EXERCÍCIO	QUANTIDADE ANUAL DEMANDADA	ANUAL ESTIMADO
1	CUSTEIO - 33904011 - Suporte de Infraestrutura de TIC	2022 em diante	12 meses por ano	R\$ 2.004.897,31
2	CUSTEIO - 33904011 - Suporte de Infraestrutura de TIC	2022 em diante	12 meses por ano	R\$ 2.444.238,44
3	CUSTEIO - 33904011 - Suporte de Infraestrutura de TIC	2022 em diante	12 meses por ano	R\$ 1.522.231,32
			<b>Valor total estimado para o contrato:</b>	<b>R\$ 5.971.367,08</b>

## 18. Benefícios a serem alcançados com a contratação

Identificação tempestiva e proativa de riscos e falhas que possam comprometer a qualidade dos serviços disponibilizados, por meio da central de monitoramento contratada;

Disponibilidade de atendimento em regime ininterrupto para reparo e ajustes da infraestrutura relacionada aos serviços finalísticos;

Cumprimento aos requisitos de disponibilidade da informação, dos serviços e das soluções de TIC relacionadas ao ambiente de assinatura avançada;

Garantia de restauração tempestiva da operação normal dos serviços corporativos de TI, como mínimo de impacto nos processos de negócios do Instituto, obedecidos os padrões e níveis mínimos de serviço;

Garantia do nível adequado de segurança, integridade e consistência dos dados manipulados e armazenados no centro de dados do ITI relativo ao escopo da contratação (Assinaturas Avançadas);

Resolução de problemas de acordo com Níveis Mínimos de Serviço, de modo que se amplie o nível de satisfação quanto aos serviços prestados.

## 19. Providências a serem Adotadas

Elaborar TR;

Avaliar TR com equipes e gestores;

Realizar análise de riscos;

Encaminhar documentação para jurídico;

Ajustar, eventualmente, documentos;

Encaminhar processo para licitação.

## 20. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

### 20.1. Justificativa da Viabilidade

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.

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.

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

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.

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

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

## 21. Responsáveis

JOSÉ RODRIGUES GONÇALVES JÚNIOR

Integrante Requisitante

MARCELO FENOLL RAMAL

Integrante Técnico

## Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Anexo - Catálogo de serviços de TIC para assinaturas avançadas do ITI.docx (87.78 KB)