

INSTITUTO NAC. DE TECNOLOGIA DA INFORMAÇÃO

Estudo Técnico Preliminar 6/2026**1. Informações Básicas**

Número do processo: 00100.002198/2025-02

2. Descrição da necessidade**2.1. Contextualização**

2.1.1. O presente Estudo Técnico Preliminar (ETP) tem por objetivo analisar a contratação de serviços técnicos especializados de Tecnologia da Informação e Comunicação (TIC), no âmbito do Instituto Nacional de Tecnologia da Informação (ITI), visando assegurar a disponibilidade, confiabilidade, integridade e segurança da infraestrutura tecnológica para os Serviços Negociais ofertados pelo Instituto Nacional de Tecnologia da Informação (ITI) à sociedade Brasileira e providos pela Diretoria de Infraestrutura Tecnológica (DITEC) e Diretoria de Auditoria, Fiscalização e Normalização (DAFN).

2.1.2. A contratação visa garantir o funcionamento e a evolução contínua dos ambientes tecnológicos que sustentam os Serviços Negociais como: Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz), da Entidade de Auditoria do Tempo (EAT), Validador de Assinaturas Eletrônicas e do serviço de Assinatura Eletrônica Avançada (Gov.BR), em alinhamento às metas e diretrizes estabelecidas no Planejamento Estratégico e no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do ITI para o período 2023–2026.

2.1.3. Espera-se que a contratação fortaleça a capacidade institucional, promovendo a maturidade operacional e de governança em TIC, o aperfeiçoamento contínuo dos processos de gestão e o alinhamento das ações tecnológicas aos objetivos estratégicos, missão, visão e valores do Instituto, em consonância com as políticas públicas de transformação digital e as melhores práticas de gestão de serviços de TIC.

2.2. Características institucionais e das atividades finalísticas

2.2.1. O ITI é uma autarquia federal vinculada ao Ministério da Gestão e da Inovação em Serviços Públicos (MGI), com atuação em todo o território nacional, responsável por implementar, supervisionar e manter a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), nos termos da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

2.2.2. Como Autoridade Certificadora Raiz (AC-Raiz) da ICP-Brasil, o ITI exerce papel estratégico na confiança digital do Estado, sendo responsável pela emissão, controle e auditoria dos certificados digitais das ACs de 1º nível, garantindo a validade jurídica das assinaturas eletrônicas e a integridade das transações digitais.

2.2.3. O Instituto também mantém a Entidade de Auditoria do Tempo (EAT), que fornece o serviço oficial de carimbo de tempo, e atua como órgão central na formulação de políticas, normas e padrões de certificação digital e confiança eletrônica.

2.2.4. No contexto da transformação digital do Governo Federal, o ITI expandiu seu escopo de atuação, tornando-se um órgão habilitador da assinatura eletrônica avançada, prevista na Lei nº 14.063/2020, integrando seus serviços à Plataforma gov.br, em apoio direto à Secretaria de Governo Digital. Essa função reforça seu papel como provedor de infraestrutura crítica para autenticação segura de cidadãos, empresas e órgãos públicos.

2.2.5. A DITEC é responsável por planejar, implantar, operar e evoluir a infraestrutura tecnológica que suporta as atividades institucionais do ITI. Sua atuação abrange os ambientes de data center, redes, servidores, bancos de dados, sistemas operacionais, segurança da informação e monitoramento de desempenho, garantindo a disponibilidade, integridade e continuidade operacional dos serviços prestados pelo Instituto.

2.2.6. A DAFN atua em áreas cruciais para a missão do ITI, especialmente no que tange à segurança e à credibilidade dos serviços digitais no país. É a diretoria responsável por planejar, coordenar, supervisionar, executar, avaliar e controlar as atividades de auditoria, fiscalização e normalização no âmbito da ICP-Brasil.

2.2.7. As atividades desempenhadas estão diretamente associadas à execução da missão institucional do ITI, sendo essenciais para o cumprimento de suas funções legais e regulatórias. A criticidade de suas operações exige ambientes de alta disponibilidade, segurança criptográfica e conformidade com padrões internacionais de auditoria e governança, como WebTrust, ISO/IEC 27001:2022 e ISO/IEC 20000-1:2020.

2.2.8. A infraestrutura tecnológica do ITI é um ativo estratégico para a soberania digital do Estado brasileiro, sustentando sistemas críticos de certificação, auditoria e autenticação digital que impactam diretamente a integridade dos serviços públicos e das transações eletrônicas. Diante da relevância institucional e das exigências operacionais, é essencial que essa infraestrutura seja moderna, resiliente, segura e continuamente aprimorada,

garantindo o cumprimento da missão do Instituto e consolidando sua posição como referência em confiança digital e inovação, em alinhamento com os princípios da governança pública e da transformação digital.

2.3. Histórico e necessidade

2.3.1. Ao longo de sua trajetória, o Instituto estruturou sua operação tecnológica com base em contratações especializadas de serviços de TIC, que garantem a sustentação da infraestrutura e a segurança dos sistemas de certificação digital, em atendimento às normas da Medida Provisória nº 2.200-2/2001, da Lei nº 14.063/2020 e dos padrões WebTrust e DOC-ICP.

2.3.3. Nos últimos anos, contratos distintos foram utilizados para o suporte às operações tecnológicas do ITI. Eles atendem à necessidade de sustentação de infraestrutura, administração de servidores, redes e bancos de dados, segurança da informação e auxílio na auditoria técnica, garantindo a conformidade dos ambientes com os requisitos normativos da ICP-Brasil e os critérios de auditoria internacional WebTrust. Os vigentes são

2.3.3.1. Contrato Administrativo ColaboraGOV/MGI nº 06/2022 (SEI/ITI nº 0761441)

- i. Processo SEI/ITI nº 00100.002376/2025-97;
- ii. Empresa: LOGIKS CONSULTORIA E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA - CNPJ/MF nº 07.696.132/0001-49;
- iii. Data e Vigência: O posicionamento do ITI como contratante se deu por adesão ao ColaboraGOV/MGI. Firmado em 19/08/2022, com prazo de vigência até 19/08/2026.
- iv. Objeto: “O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação do tipo serviços de consultoria técnica especializada para apoio a Gestão e Governança de TI, por um período de 12 (doze) meses, sendo renováveis por interesse das partes, até o limite de 60 (sessenta) meses, com base no ar go 57, II, da Lei 8.666, de 1993, que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital”.

2.3.3.2. Contrato Administrativo nº 10/2022 (SEI/ITI nº 0570581)

- i. Processo SEI/ITI nº: 00100.003688/2021-94;
- ii. Empresa DSS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO LTDA - CNPJ nº 03.627.226-0001/05;
- iii. Data e Vigência: Firmado em agosto de 2022, com prazo de vigência de vinte e quatro (24) meses, prorrogável conforme previsto no Termo de Referência e contrato, a contar da data de assinatura do Diretor Presidente do ITI, podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses
- iv. Objeto: “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), para atendimento das necessidades no âmbito do Instituto Nacional de Tecnologia da Informação - ITI/PR, conforme condições, quantidades e exigências estabelecidas neste instrumento.”

2.3.4. Esses instrumentos possibilitaram avanços significativos na estabilidade, confiabilidade e segurança da infraestrutura tecnológica do Instituto. Contudo, a evolução do papel institucional do ITI, associada às novas atribuições estratégicas decorrentes da Política de Governo Digital (Decreto nº 10.332/2020), impõe desafios tecnológicos e operacionais adicionais, que ultrapassam o escopo das contratações vigentes.

2.3.5. Apesar de cumprirem funções específicas, esses contratos operam de forma fragmentada, sem integração operacional, técnica e de governança. Tal modelo resulta em:

- Dificuldade de correlação entre eventos de infraestrutura e segurança, comprometendo a gestão proativa de incidentes e vulnerabilidades;
- Ausência de um modelo de governança unificado, com métricas e indicadores de desempenho que permitam aferição da eficiência operacional;
- Baixa visibilidade consolidada sobre desempenho, capacidade e disponibilidade dos ambientes críticos;
- Dependência contratual dispersa, dificultando a priorização de ações de melhoria e a execução de planos estruturantes previstos no PDTIC.

2.3.6. O Planejamento Estratégico 2023–2026 e o PDTIC 2023–2026 apontam expressamente a necessidade de ampliar a capacidade institucional de operação, automação e monitoramento dos ambientes de TIC, de modo a permitir a expansão segura dos serviços digitais sob responsabilidade do ITI, com ênfase nos seguintes eixos:

- Governança e segurança da informação, com aderência às normas ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 20000-1:2020;
- Alta disponibilidade e resiliência operacional dos serviços da AC-Raiz e da EAT;
- Melhoria contínua dos processos de gestão de serviços de TIC, segundo o modelo ITIL v4;
- Adoção de soluções automatizadas de monitoramento, observabilidade e gestão de capacidade;
- Aprimoramento da maturidade de governança e alinhamento entre as áreas técnicas e estratégicas da Instituição.

2.3.7. A experiência acumulada na gestão dos contratos vigentes demonstra que, embora o modelo atual tenha garantido a continuidade dos serviços, ele não contempla integralmente as novas necessidades tecnológicas e estratégicas identificadas, em especial no que se refere à integração entre infraestrutura e segurança, à adoção de métricas de desempenho (NMS) e à evolução dos processos de governança e conformidade.

2.3.8. Dessa forma, a nova contratação se faz necessária para consolidar a transição para um modelo de serviços orientado a resultados, conforme preconizado pela Portaria SGD/MGI nº 1.070/2023, que estabelece as diretrizes para contratações de serviços de operação de infraestrutura e segurança de TIC, baseadas em indicadores mensuráveis de desempenho e qualidade.

2.3.9. Além de atender às recomendações do PDTIC, a contratação permitirá elevar a maturidade dos processos operacionais e de governança, garantindo o cumprimento de metas institucionais vinculadas à segurança da informação, transformação digital e eficiência administrativa, em consonância com a missão, visão e valores organizacionais do ITI.

2.3.10. Em síntese, a nova contratação é estratégica e estruturante: visa não apenas garantir a continuidade dos serviços críticos, mas também promover a modernização tecnológica e a melhoria contínua dos processos de gestão de TIC, assegurando a resiliência, a conformidade e a sustentabilidade da infraestrutura que sustenta a confiança digital no Brasil.

2.4. Motivação e Justificativa

2.4.1. A presente contratação é motivada pela necessidade de assegurar a continuidade, a confiabilidade e a evolução da infraestrutura tecnológica crítica sob responsabilidade do ITI, essencial à sustentação dos serviços da ICP-Brasil, da EAT e das plataformas de Assinatura Eletrônica Avançada (Gov.BR) e Validar, inclusive o fornecimento via API (Application Programming Interface).

2.4.2. O Planejamento Estratégico 2023–2026 estabelece, entre seus objetivos e projetos estruturantes, o compromisso de “fortalecer a infraestrutura tecnológica, a segurança da informação, a comunicação e os serviços tecnológicos”, destacando como ação prioritária “adotar medidas para melhoria da infraestrutura de TIC de modo a mitigar os riscos de descontinuidade dos processos”. Essa diretriz contempla iniciativas como “renovar garantia dos ativos de infraestrutura e segurança, expandir licenças e implantar mecanismos de alta disponibilidade e recuperação de desastres”, reafirmando a natureza crítica da área tecnológica para o cumprimento da missão institucional do ITI.

2.4.3. O PDTIC 2023–2026, por sua vez, define o plano como “instrumento de diagnóstico, planejamento e gestão dos recursos e processos de TIC, com o objetivo de atender às necessidades finalísticas e de informação de um órgão ou entidade para um determinado período”. O documento reforça que sua finalidade é “permitir o direcionamento das ações e projetos de TIC de todas as unidades organizacionais do ITI, a fim de garantir eficiência e eficácia na gestão de TIC”, além de assegurar a coerência entre as ações táticas de tecnologia e os objetivos estratégicos da Instituição.

2.4.4. O mesmo PDTIC, ao apresentar o referencial estratégico de TIC, estabelece como missão “prover soluções em TIC que atendam às necessidades e políticas do ITI, promovendo o acesso à informação e a prestação de serviços digitais à sociedade, com segurança e tempestividade” e como visão “ser reconhecida como provedora de soluções inovadoras em TIC, contribuindo para que os objetivos estratégicos sejam alcançados por meio da gestão e melhoria contínua dos serviços digitais oferecidos”.

2.4.5. Esses direcionadores deixam claro que a contratação de serviços técnicos especializados de TIC é condição indispensável para cumprimento da estratégia institucional. As contratações vigentes, estruturadas em modelos segmentados de sustentação e segurança, garantem a manutenção operacional mínima, porém não abrangem as novas demandas de integração, automação e governança requeridas pela ampliação das responsabilidades do Instituto e pelo contexto de transformação digital do Estado brasileiro.

2.4.6. Diante desse cenário, a adoção de um modelo de prestação de serviços orientado a resultados, com Níveis Mínimos de Serviço (NMS) e indicadores de desempenho, representa não apenas um aprimoramento técnico, mas uma evolução na gestão pública de TIC. Tal modelo, conforme orienta a Portaria SGD/MGI nº Portaria SGD/MGI nº 1.070/2023 e suas alterações, busca “gerar incentivos para que os contratados prestem serviços associados ao uso de recursos tecnológicos que forneçam agilidade e qualidade adequadas às condições exigidas”.

2.4.7. Portanto, esta contratação é estruturante e estratégica, uma vez que permitirá ao ITI:

- consolidar um modelo de gestão de TIC baseado em governança, desempenho e melhoria contínua;
- garantir a resiliência e a segurança da infraestrutura tecnológica sob sua responsabilidade;
- atender de forma direta às metas institucionais expressas no Planejamento Estratégico e no PDTIC 2023–2026;
- e sustentar, de forma confiável, as operações que asseguram a confiança digital do Estado brasileiro.

2.4.8. Em síntese, a motivação que fundamenta esta contratação é o compromisso de elevar a maturidade tecnológica e operacional do ITI, transformando a infraestrutura atual em uma base sustentável, segura e alinhada às melhores práticas internacionais de gestão e governança de TIC.

2.5. Vinculação da necessidade e motivação

2.5.1. A necessidade identificada está diretamente associada à execução da missão institucional do ITI, que consiste em “garantir a confiança nas transações eletrônicas e promover a transformação digital com segurança jurídica, confiabilidade e transparência”.

2.5.2. O Planejamento Estratégico 2023–2026 estabelece como objetivo estratégico “fortalecer a infraestrutura tecnológica, a segurança da informação, a comunicação e os serviços tecnológicos”, o que exige a ampliação da capacidade técnica e operacional para assegurar a continuidade e a evolução dos serviços sob sua responsabilidade.

2.5.3. O PDTIC 2023–2026 reforça essa diretriz ao definir como missão da área de TIC “prover soluções em TIC que atendam às necessidades e políticas do ITI, promovendo o acesso à informação e a prestação de serviços digitais à sociedade, com segurança e tempestividade”, e como visão “ser reconhecida como provedora de soluções inovadoras em TIC, contribuindo para que os objetivos estratégicos sejam alcançados por meio da gestão e melhoria contínua dos serviços digitais oferecidos”.

2.5.4. Dessa forma, a motivação e a necessidade encontram-se plenamente vinculadas: a contratação é condição essencial para a modernização, automação e resiliência da infraestrutura tecnológica do ITI, além de ser um instrumento de aperfeiçoamento da governança de TIC e de cumprimento dos objetivos estratégicos estabelecidos nos documentos de planejamento institucional.

2.6. Os Eixos de Atuação dos Serviços das Unidades Organizacionais

2.6.1. A DITEC é responsável por planejar, implementar, operar e manter a infraestrutura tecnológica do ITI, assegurando o suporte técnico necessário à execução de suas atividades finalísticas e estratégicas. Suas ações estão estruturadas em três eixos principais de atuação, que abrangem as atividades essenciais ao funcionamento contínuo da ICP-Brasil, da EAT e dos serviços digitais sob responsabilidade do Instituto.

- I. O primeiro está relacionado à infraestrutura e operações tecnológicas, englobando a administração de servidores, sistemas operacionais, bancos de dados, redes e componentes de conectividade. Esse eixo visa garantir a disponibilidade, o desempenho e a estabilidade dos ambientes críticos, assegurando a execução ininterrupta dos serviços institucionais.
- II. Já o segundo corresponde à segurança da informação e conformidade, abrangendo as atividades de proteção dos ambientes tecnológicos, controle de acesso, monitoramento de eventos e gestão de incidentes de segurança. Também contempla o atendimento aos requisitos de conformidade com normas e auditorias nacionais e internacionais, como WebTrust, ISO/IEC 27001, ISO/IEC 22301 e DOC-ICP, que sustentam a confiabilidade e a segurança jurídica da atuação do ITI.
- III. O terceiro eixo refere-se à governança e melhoria contínua dos serviços de TIC, orientado à padronização e otimização dos processos de gestão, em conformidade com as boas práticas do ITIL v4, COBIT 2019 e ISO/IEC 20000-1. Esse eixo tem como finalidade elevar o nível de maturidade operacional, aprimorar a gestão de desempenho e promover a evolução tecnológica contínua, em alinhamento ao Planejamento Estratégico e ao PDTIC 2023–2026.

2.6.1.1. Esses eixos de atuação representam a base técnica e operacional da DITEC e garantem que os serviços de TIC do ITI sejam executados de forma eficiente, segura e aderente às políticas públicas de transformação digital, contribuindo para a manutenção da confiança nas transações eletrônicas e o fortalecimento da infraestrutura tecnológica do Estado brasileiro.

2.6.2. A DAFN é central nas atividades de controle e conformidade. Suas responsabilidades incluem:

- Planejamento e Execução de Auditoria e Fiscalização: A Diretoria planeja, coordena, supervisiona, executa, avalia e controla as atividades de auditoria e fiscalização relacionadas à ICP-Brasil e aos sistemas da Carteira de Identidade Nacional e do Sistema de Identificação Civil do Brasil.
- Auditorias Específicas: A DAFN/CGAFI (Coordenação-Geral de Auditoria e Fiscalização) pode realizar auditorias pré-operacionais e operacionais em qualquer entidade que integre ou queira integrar a ICP-Brasil, utilizando servidores qualificados do seu quadro.
- Fiscalização de Entes: Propõe à Cefic os regulamentos, a revisão e a atualização referentes aos processos de auditoria e fiscalização de entes públicos e privados sobre sistemas biométricos, de personalização e de gráficas no âmbito da expedição da CIN. A fiscalização visa garantir que as exigências de auditorias pré-operacionais e anuais, atendimento de denúncias e combate a fraudes sejam cumpridas.
- Aplicação de Sanções: A DAFN é responsável por propor e/ou aplicar sanções e penalidades às entidades integrantes da ICP-Brasil, conforme a legislação.

2.6.2.1. Normalização e Regulação - No papel de normalização, a DAFN garante que as operações do ITI e da ICP-Brasil sigam os padrões técnicos e legais: Compete à DAFN fornecer subsídios para a elaboração de propostas, revisão e atualização de normas técnicas e operacionais de competência do Comitê Gestor da ICP-Brasil e do ITI. Além disso, elabora propostas de revisão das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil e pela Cefic.

2.6.2.2. Credenciamento e Gestão de Riscos - A DAFN também desempenha um papel fundamental na gestão da cadeia de confiança e na infraestrutura de auditoria:

- Credenciamento de Entidades: Atua como credenciador de entidades, tanto públicas quanto privadas, na ICP-Brasil, e também de empresas de auditoria ou auditores independentes para a prestação de serviços ao Comitê Gestor da ICP-Brasil, à Cefic e a instâncias de governança do ITI.
- Gerenciamento de Riscos e Conformidade: Gerencia os riscos sobre a confiabilidade da ICP-Brasil decorrentes das atividades de credenciamento de sua competência. Entidades devem apresentar à DAFN documentos de conformidade, como apólices de seguro e certificados para equipamentos, para análise.

2.6.2.3. Suporte Operacional e Capacitação - A Diretoria também atua no apoio técnico e capacitação:

- Rastreabilidade e Identificação: Planeja, coordena, supervisiona e implementa os meios técnicos para a rastreabilidade e a identificação de objetos nos diversos escopos de serviços do ITI.
- Capacitação: Planeja, coordena e estabelece o conteúdo técnico, legal e operacional necessários à capacitação dos agentes de registro.
- Gestão de TIC para a Área: Administra as atividades relacionadas à gestão dos recursos de Tecnologia da Informação e Comunicação (TIC) para as ações que envolvam auditoria, fiscalizações ou normalização no âmbito da ICP-Brasil.

2.6.2.4. Adicionalmente, a diretoria é uma das unidades organizacionais do ITI listadas na estrutura de TIC, juntamente com suas coordenações: Coordenação-Geral de Auditoria e Fiscalização (CGAFI) e Coordenação-Geral de Normalização e Pesquisa (CGNPE).

2.7. Natureza da Utilização

2.7.1. A utilização dos serviços objeto desta contratação possui natureza continuada e essencial, voltada à sustentação, operação e evolução da infraestrutura tecnológica que dá suporte às atividades institucionais e finalísticas do ITI. Esses serviços são indispensáveis à manutenção da ICP-Brasil, da EAT e das plataformas de assinatura eletrônica avançada (Gov.br), pilares técnicos da confiança digital do Estado brasileiro.

2.7.2. Os serviços a serem contratados serão utilizados de forma integrada nas operações técnicas, de segurança e de governança da infraestrutura do ITI, abrangendo, entre outros, os seguintes tipos:

2.7.2.1. Administração e operação de servidores, bancos de dados, sistemas operacionais e redes

- Envolve o gerenciamento técnico e contínuo dos ambientes computacionais que suportam as aplicações institucionais e os sistemas de certificação digital.
- Essa atividade é essencial para garantir a disponibilidade, o desempenho e a estabilidade dos ambientes críticos do ITI, como os servidores da AC-Raiz e da EAT, que devem operar com níveis de disponibilidade superiores a 99,9%.
- A falta de gestão e operação especializada desses recursos impactaria diretamente a emissão, validação e auditoria de certificados digitais, além de comprometer a conformidade com as normas da ICP-Brasil e as auditorias WebTrust, que exigem evidências técnicas de controle e continuidade.

2.7.2.2. Gestão e controle de segurança da informação

- Compreende as atividades de proteção, detecção e resposta a incidentes de segurança, além da administração de identidades, acessos e permissões nos ambientes críticos.
- A execução dessas atividades é fundamental para prevenir vulnerabilidades, ataques cibernéticos e acessos indevidos, assegurando a integridade dos dados e a rastreabilidade das ações.
- A gestão de segurança, no contexto do ITI, possui caráter normativo e jurídico, pois garante a conformidade com os padrões DOC-ICP, a ISO/IEC 27001 e a Portaria SGD/MGI nº 6.680/2024, além de sustentar a credibilidade do Instituto perante as entidades credenciadas e auditoras da ICP-Brasil.
- A ausência de controles e monitoramento contínuo de segurança exporia o ITI a riscos operacionais e de imagem institucional, afetando diretamente a confiança nas transações eletrônicas.

2.7.2.3. Monitoramento e observabilidade dos ambientes tecnológicos

- Trata-se do conjunto de atividades destinadas à detecção proativa de falhas, degradações e vulnerabilidades, por meio de ferramentas automatizadas de observabilidade, monitoramento de desempenho e correlação de eventos.
- A implementação desse tipo de serviço é necessária para a manutenção da visibilidade integral sobre a operação dos ativos críticos, permitindo respostas ágeis e preditivas frente a incidentes e indisponibilidades.
- Além de reduzir o tempo médio de detecção e resposta (MTTD/MTTR), o monitoramento contínuo contribui para aumentar a resiliência operacional e o cumprimento dos Níveis Mínimos de Serviço (NMS) definidos contratualmente.
- Essa capacidade é estratégica para o ITI, pois garante previsibilidade e controle sobre a infraestrutura, sustentando a continuidade das operações da ICP-Brasil e das plataformas Gov.BR.

2.7.2.4. Gestão da capacidade e continuidade de serviços

- Abrange o planejamento e o controle do uso dos recursos computacionais — como processamento, armazenamento e rede —, além da implementação de estratégias de alta disponibilidade, redundância e recuperação de desastres (DRP/BCP).
- Essa gestão é indispensável para que o ITI possa antecipar gargalos, dimensionar adequadamente seus ambientes e assegurar a continuidade dos serviços mesmo em situações de falha ou contingência.
- O correto gerenciamento da capacidade evita a degradação de desempenho, o esgotamento de recursos e o risco de interrupções que comprometam a certificação digital e a validação temporal, que são serviços de interesse nacional.
- A continuidade operacional, nesse contexto, é uma obrigação técnica e estratégica da DITEC, garantindo que os ambientes estejam sempre disponíveis e em conformidade com as políticas de segurança da informação e com os padrões da ICP-Brasil.

2.7.2.5. Apoio à governança e à melhoria contínua dos processos de TIC

- Compreende o suporte técnico e metodológico à padronização, documentação e evolução dos processos de gestão de TIC, com base em boas práticas reconhecidas, como ITIL v4, COBIT 2019 e ISO/IEC 20000-1.
- Essas atividades visam elevar o nível de maturidade dos processos operacionais e gerenciais, promovendo maior eficiência, controle e transparência nas ações de tecnologia.
- O apoio à governança é essencial para garantir que os serviços de TIC sejam prestados com foco em resultados mensuráveis, alinhados à política de transformação digital da Administração Pública Federal e aos objetivos estratégicos do ITI.
- Além disso, possibilita a implementação de um modelo de gestão baseado em indicadores e NMS, conforme previsto na Portaria SGD/MGI nº 6.680/2024, permitindo à Instituição adotar uma abordagem orientada à melhoria contínua e à agregação de valor institucional.

2.7.3. A utilização dos serviços apresenta, portanto, caráter técnico, estratégico e estruturante, constituindo um elemento indispensável à manutenção da operação segura, estável e ininterrupta dos sistemas críticos do Instituto.

2.7.4. Esclarecimento quanto ao público atendido e à adequação ao modelo da Portaria SGD/MGI nº 1.070/2023. Para os fins desta contratação, entende-se por "usuários" os usuários de TIC internos do ITI — servidores, colaboradores e equipes das unidades do Instituto —, cujo atendimento se dá por meio da Central de Serviços de TIC (ITSM), com abertura, triagem e tratamento de chamados técnicos, conforme o Catálogo de Serviços (Apêndice II) e as Equipes Técnicas (Apêndice III). A contratação não compreende o atendimento ao usuário final externo (o cidadão ou o titular de certificado da ICPBrasil), o qual é prestado por outros meios e canais institucionais do ITI — sendo esse o alcance da observação registrada no Documento de Formalização da Demanda. Esse recorte é plenamente aderente ao modelo da Portaria SGD/MGI nº 1.070/2023, que disciplina os serviços de operação

de infraestrutura e de atendimento aos usuários de TIC do órgão: foram adotadas as categorias de serviço pertinentes do Anexo I (seção 2.3.2), na forma detalhada no item 7.8 deste Estudo, ao passo que eventuais categorias voltadas ao atendimento ao usuário final externo não se aplicam ao objeto e, por isso, não foram incorporadas, sem prejuízo da adequação ao modelo.

2.7.5. Ao consolidar esses serviços sob um modelo integrado e orientado por NMS, o ITI reforça sua capacidade de sustentar a confiança digital do Estado brasileiro, assegurando que suas infraestruturas e processos tecnológicos operem de forma resiliente, segura e alinhada aos objetivos estratégicos de “garantir a confiança nas transações eletrônicas e promover a transformação digital com segurança jurídica, confiabilidade e transparência”.

2.8. Alinhamento Estratégico

2.8.1. Alinhamento com a Estratégia Federal de Governo Digital (EFGD) - A contratação de serviços de operação de infraestrutura de TIC está diretamente ligada aos objetivos da EFGD 2024-2027 (Decreto nº 12.198/2024), pois garante a fundação tecnológica para os serviços digitais de Estado.

- **Infraestrutura de Suporte Essencial:** A contratação não se enquadra como um "serviço público digital" em si, mas sim como a infraestrutura de suporte essencial à prestação de serviços digitais críticos, como as Assinaturas Eletrônicas Avançadas do Gov.BR. A EFGD visa, entre outros, a ampliação da oferta e o aprimoramento dos serviços públicos por meio da transformação digital (OE.03).
- **Segurança e Resiliência Cibernética:** A contratação de operação de infraestrutura, com foco em alta disponibilidade e segurança reforçada, é fundamental para proteger os ativos digitais e garantir a segurança dos serviços públicos digitais no Brasil. O objeto exige especificamente monitoramento por meio de NOC (Network Operations Center) e SOC (Security Operations Center), uma medida essencial para a cibersegurança e a mitigação de riscos.
- **Conformidade Normativa:** Os serviços de operação de infraestrutura e atendimento a usuários de TIC são considerados soluções de TIC e, portanto, devem se orientar pelos dispositivos da Instrução Normativa SGD/ME nº 94, de 2022. A IN 94/2022 exige que as contratações de TIC sejam integradas à Plataforma gov.br quando visam a oferta digital de serviços públicos, e a infraestrutura em questão suporta diretamente os serviços Gov.BR.
- **Promoção da Governança:** O ITI tem competências na promoção da Infraestrutura Nacional de Dados, melhorando a governança, a privacidade, a segurança da informação e a interoperabilidade no âmbito da APF. A contratação de serviços técnicos especializados é uma ação de governança de TIC que busca eficiência e alinhamento com as políticas federais.

2.8.2. A presente contratação está plenamente alinhada aos instrumentos de planejamento e gestão institucional do ITI, em especial ao Planejamento Estratégico (2023–2026) e ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC 2023–2026), os quais orientam a atuação da área de tecnologia da informação no cumprimento da missão institucional de “garantir a confiança nas transações eletrônicas e promover a transformação digital com segurança jurídica, confiabilidade e transparência”.

2.8.3. Alinhamento com o Planejamento Estratégico do ITI - A contratação está diretamente vinculada à missão institucional do ITI, conforme o planejamento estratégico (PEI) da autarquia:

- **Missão Crítica e Essencialidade:** O ITI é a AC Raiz da ICP-Brasil e é responsável pela governança da identidade digital no Brasil (CIN). A contratação é essencial para assegurar a continuidade e a integridade dessas plataformas tecnológicas.
- **Objetivos Estratégicos (PEI):** A ação está alinhada a objetivos claros do Planejamento Estratégico Institucional:
- **DI-4:** Garantir o funcionamento do Sistema Nacional de Certificação Digital nos padrões nacionais e internacionais. A operação ininterrupta e segura da infraestrutura de TIC é o meio pelo qual se cumpre esse objetivo.
- **AL-3:** Melhorar as soluções de tecnologia da informação e comunicação mantendo-as compatíveis com as demandas institucionais. A contratação de serviços técnicos especializados de TIC é a solução de mercado para a sustentação e operação do ambiente.
- **Conformidade de Segurança:** A operação da infraestrutura deve seguir rigorosos padrões de segurança definidos em normativos como a Política de Segurança da ICP-Brasil (DOC-ICP-02), o que exige conhecimento técnico especializado e monitoramento contínuo. O objeto da contratação inclui explicitamente as categorias de Segurança de TIC e Gerenciamento de Serviços de TIC.

2.8.4. Alinhamento com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do ITI - O PDTIC (2023-2026) é o instrumento tático que norteia e acompanha a atuação da área de TIC do ITI, estando por sua vez alinhado ao PEI e à Estratégia de Governo Digital.

- **Exigência de Consonância:** Conforme a IN SGD/ME nº 94/2022, as contratações de soluções de TIC devem estar em consonância com o PDTIC do órgão. O processo de contratação demonstra esse alinhamento nos seus documentos de planejamento (ETP e TR).
- **Ações e Metas Específicas (ACTI):** ACTI-04 - Serviços especializados de suporte à infraestrutura de datacenter e de redes de dados (Nível 3) e ACTI-06 - Sustentação de serviços de assinatura eletrônica avançada.
- **Níveis de Serviço:** A ação de contratar serviços especializados visa definir o catálogo e os níveis de serviços de TIC (NEI-09) e garantir o Índice de Disponibilidade dos Serviços/Sistemas Corporativos Críticos (IDS).

2.8.5. Além disso, o mesmo planejamento aponta o aperfeiçoamento da governança institucional e a adoção de práticas de gestão orientadas a resultados como pilares do desempenho organizacional. Nesse sentido, a contratação de serviços de TIC sob o modelo de Níveis Mínimos de Serviço (NMS) e indicadores de desempenho, conforme a Portaria SGD/MGI nº 1.070/2023 e suas alterações, materializa essa diretriz, ao permitir a mensuração objetiva da qualidade e eficiência dos serviços prestados.

2.8.6. Em seu referencial de visão, o documento estabelece o propósito de “ser reconhecida como provedora de soluções inovadoras em TIC, contribuindo para que os objetivos estratégicos sejam alcançados por meio da gestão e melhoria contínua dos serviços digitais oferecidos”.

2.8.7. Alinhamento com o Plano de Contratações Anual de 2026 - O objeto da contratação está previsto no Plano de Contratações Anual de 2026, conforme tabela a seguir, bem como pode ser consultado através do link do PNCP (<https://pncp.gov.br/app/pca/04039532000193/2026>):

Tabela 2.01. Dados do PCA

ID do Item no PCA	Classe/Grupo	DFD nº	Identificador da Futura Contratação	Valor Previsto
197	162 - SERVIÇOS DE GERENCIAMENTO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC)	10/2026	243001-143/2026	R\$ 2.700.000,00

2.8.8. Alinhamento com o Plano de Logística Sustentável (PLS) — A presente contratação está alinhada ao Plano de Logística Sustentável do ITI, ciclo 2024–2026, aprovado pela Portaria ITI nº 76, de 31 de dezembro de 2024 (Processo SEI nº 00100.001004/202462), em atenção ao art. 18, § 1º, XII, da Lei nº 14.133/2021 e à IN SEGES/ME nº 58/2022. O objeto observa, em especial, o Eixo 3 do PLS ("Identificação dos objetos de menor impacto ambiental"), cuja meta é que 100% dos processos de contratação contenham critérios de sustentabilidade, bem como as diretrizes de racionalização e consumo consciente (Eixo 1) e de capacitação dos prestadores quanto ao uso eficiente de energia e água e à redução de resíduos (Eixo 6).

2.9. O modelo pretendido de contratação de sustentação de infraestrutura de TIC

2.9.1. A presente contratação, deverá ser realizada por meio de modelo de pagamento fixo mensal, vinculada ao atendimento de níveis mínimos de serviços previamente estabelecidos, conforme quantidades e perfis profissionais mínimos previstos em ordens de serviços, de acordo com a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, que institui o modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal, e estabelece, em seu Capítulo I, que:

"Art. 2º A contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação deverá ser realizada por meio de modelo de pagamento fixo mensal, vinculada ao atendimento de níveis mínimos de serviços previamente estabelecidos, conforme quantidades e perfis profissionais mínimos previstos em ordens de serviços. (Alterado pela Portaria SGD/MGI nº 6.680, de 04 de outubro de 2024)

Parágrafo único. O modelo não se configura como de dedicação exclusiva de mão de obra, contratação por homem/hora e tampouco por postos de trabalho.

Art. 3º O modelo de contratação descrito no Anexo I desta Portaria é de utilização obrigatória para a contratação de serviços de operação de infraestrutura e atendimento a usuários de tecnologia da informação e comunicação."

2.9.2. O modelo é composto de ações de compreensão do ambiente de TIC, levantamento de dados históricos para fundamentar a estimativa dos perfis profissionais e seus quantitativos, necessários para a prestação do serviço, estabelecendo um modelo de pagamento fixo mensal vinculado ao atendimento a Níveis Mínimos de Serviço (NMS).

2.9.3. A Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos publicou as Portarias SGD/MGI nº 6.680, de 04 de outubro de 2024, SGD/MGI nº 6.055, de 26 de agosto de 2025, e Portaria SGD/MGI nº 5.921, de 22 de julho de 2026. Estas portarias incluem anexos e promovem alterações na portaria SGD/MGI nº 1.070, de 1º de junho de 2023. Diante desse cenário, a Equipe de Planejamento da Contratação empenhou todos os esforços para adequar o presente estudo ao modelo estabelecido pela portaria, garantindo a conformidade com as novas diretrizes. Assim, sempre que a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, for mencionada neste Estudo, serão consideradas também as alterações introduzidas por estas portarias.

2.9.4. Este modelo propõe a remuneração a partir da aferição dos níveis de serviços, gerando um incentivo para a disponibilidade ininterrupta, o que, por sua vez, favorece a excelência no acesso aos serviços de TIC da Administração Pública Federal (APF) por parte do usuário, conferindo, assim, agilidade e presteza aos processos institucionais que se utilizam de tais serviços. Assim sendo, diferentemente dos modelos que utilizam remuneração por unidades de serviços ou por chamados atendidos, o risco de haver necessidade de negociação de otimização de atividades rotineiras é reduzido, vez que a própria CONTRATADA tem interesse na melhoria dos processos. O modelo de contratação proposto ajuda na redução do esforço de fiscalização e privilegia o foco de atenção dos gestores naquilo que é relevante.

2.9.5. A modalidade de contratação proposta na Portaria SGD/MGI nº 1.070, de 1º de junho de 2023 apresenta diversas vantagens à instituição, destacando-se:

- Garantia da disponibilidade, integridade, resiliência e segurança de recursos tecnológicos necessários para a sustentação dos serviços baseados em TIC da DITEC/ITI.
- Maior transparência, agilidade e previsibilidade no processo de planejamento da contratação, com a utilização de valores padronizados para estimativa de preços dos perfis profissionais, bem como definição do valor de referência da contratação.
- A execução dos serviços está vinculada a critérios objetivos de qualidade e resultados.
- Adoção de práticas de gerenciamento de serviços descritas na série ABNT NBR ISO 20.000:2020, bem como em práticas ágeis de DevSecOps.

2.9.6. Assim, a utilização da Portaria SGD/MGI nº 1.070/2023 (e suas antecessoras, como a Portaria SGD/ME nº 6.432/2021) é uma ação de governança. Este modelo foi criado em resposta às recomendações do TCU (Acórdãos nº 2.037/2019 e nº 1.508/2020), mitigando os riscos de sobrepreço e

fiscalização deficiente associados a modelos anteriores (como UST). Ao adotar o modelo 1.070, o ITI cumpre a exigência de aderência a Modelos Padronizados e Recomendações de Controle.

2.10. Conclusão

2.10.1. A contratação atende diretamente aos eixos estratégicos “Governança e Segurança da Informação” e “Infraestrutura e Sustentabilidade Tecnológica”, previstos no Planejamento Estratégico, além de viabilizar a execução das ações e projetos definidos no PDTIC 2023–2026.

2.10.2. Ao promover a integração entre infraestrutura, segurança e governança, a iniciativa fortalece a capacidade institucional e assegura a aderência das soluções tecnológicas aos objetivos estratégicos do ITI, contribuindo para uma gestão pública mais digital, eficiente e transparente.

2.10.3. Os serviços solicitados neste estudo são de natureza continuada, dada a sua essencialidade para a finalidade pública de forma permanente e contínua. Em face do exposto, esta equipe de planejamento da contratação posiciona-se conclusivamente pela viabilidade e adequação desta contratação para o atendimento da necessidade aqui descrita e, consequentemente, para a salvaguarda dos serviços críticos prestados à sociedade brasileira pelo ITI.

2.10.4. Levando em consideração a quantidade de atendimentos realizados todos os meses e com o objetivo de manter o pleno funcionamento dos recursos e serviços do ambiente de TIC e melhorar a qualidade dos serviços prestados aos seus usuários, de forma a apoiá-los tempestivamente nos processos de trabalho e em suas atividades finalísticas, garantindo o pronto atendimento às demandas, torna-se indispensável à contratação dos serviços, uma vez que a paralisação do fornecimento dos mesmos poderá trazer prejuízos à Administração Pública e à sociedade.

2.10.5. Alinha-se que o objeto da contratação é o de serviços técnicos especializados de operação de infraestrutura e atendimento a usuários de tecnologia da informação e comunicação - TIC, não tratando-se de serviços dentre os dispostos no art. 3º do Decreto nº 9.507, de 2018, inclusive a gestão de processos de TIC e a gestão de segurança da informação. Registra-se, portanto, que a presente contratação não incide nas hipóteses vedadas pelos Arts. 3º, 4º e 5º da IN/SGD 94/2022.

3. Área requisitante

Área Requisitante	Responsável
Diretoria de Infraestrutura Tecnológica (DITEC)	José Rodrigues Gonçalves Júnior

4. Necessidades de Negócio

4.1. A presente contratação é motivada pela necessidade de garantir a disponibilidade, confiabilidade, integridade e segurança da infraestrutura para os Serviços Negociais ofertados pela de Diretoria de Infraestrutura Tecnológica (DITEC) e pela Diretoria de Auditoria, Fiscalização e Normalização (DAFN).

4.2. Dimensão Estratégica: Alinhamento e Governança - A contratação visa fortalecer a governança tecnológica e a maturidade institucional, atendendo às diretrizes de modernização e eficiência do Governo Federal. As necessidades de negócio estratégicas são:

- **Aderência à Legislação e Normativos:** Cumprir os requisitos da Portaria SGD/MGI nº 1.070/2023 e demais normas vigentes que exigem contratações orientadas a resultados e uso racional de recursos públicos.
- **Alinhamento Institucional:** Cumprir as metas do PDTIC 2023–2026, que determinam a necessidade de "adotar medidas para melhoria da infraestrutura de TIC de modo a mitigar os riscos de descontinuidade dos processos" e "promover a gestão integrada e eficiente dos serviços de tecnologia".
- **Sustentação da Missão Finalística:** Assegurar a confiança, autenticidade e integridade das transações eletrônicas realizadas no âmbito da ICP-Brasil (Autoridade Certificadora Raiz, EAT e Assinaturas Eletrônicas), essenciais para a missão do ITI.
- **Integração e Eficiência Administrativa:** Promover a integração dos serviços de infraestrutura e segurança sob um único contrato orientado a Nível Mínimo de Serviço (NMS), reduzindo a dependência de contratos fragmentados e aumentando a sinergia entre as áreas.

4.3. Dimensão Operacional: Continuidade e Segurança - A dimensão operacional foca em garantir a estabilidade e a resiliência dos ambientes tecnológicos de missão crítica e dos serviços públicos digitais. Os macroprocessos a serem garantidos pela contratação são:

- **Sustentação e Disponibilidade de Missão Crítica:** Administrar e operar servidores, bancos de dados, redes e sistemas operacionais, garantindo a performance e alta disponibilidade dos sistemas finalísticos (AC-Raiz, EAT e Assinaturas Eletrônicas).
- **Segurança e Conformidade Regulatória:** Assegurar a gestão da segurança da informação (prevenção, detecção e resposta a incidentes), o cumprimento dos requisitos DOC-ICP e ISO/IEC 27001, e a sustentação da conformidade com os requisitos de auditoria WebTrust.
- **Continuidade de Negócio e Recuperação:** Gerir a capacidade e continuidade de serviços, assegurando redundância e a pronta recuperação de desastres (DRP/BCP), conforme diretrizes da ICP-Brasil e padrões internacionais (ISO/IEC 22301), garantindo a continuidade do negócio.

- **Gestão Proativa e Observabilidade:** Implementar monitoramento e observabilidade de ambientes com uso de soluções integradas que permitam análise proativa de eventos, correlação de incidentes e detecção de anomalias.

5. Necessidades Tecnológicas

5.1. A prestação de serviços deverá estar estruturada em eixos interconectados, garantindo a evolução da maturidade tecnológica e a integração com as metas estratégicas da Instituição:

5.1.1. **Sustentação, Operação e Eficiência da Infraestrutura** - Esses serviços deverão sustentar a operação de forma resiliente e contínua, assegurando que as plataformas críticas mantenham integridade e estabilidade frente ao aumento de demanda e à complexidade dos ecossistemas digitais. A contratação deverá prover:

- **Administração Técnica e Manutenção:** Gestão e manutenção de servidores físicos e virtuais, equipamentos de rede, sistemas operacionais, bancos de dados, armazenamento, backup e conectividade, garantindo a atualização e o desempenho adequado de hardware e software.
- **Virtualização e Nuvem:** Considerar a utilização de tecnologias de virtualização e computação em nuvem para otimização de recursos, escalabilidade e flexibilidade, alinhadas às necessidades do Órgão.
- **Continuidade e Recuperação de Dados (BCP/DRP):** Realização de backups periódicos e a implementação e execução periódica de planos de continuidade e recuperação de desastres, essenciais para garantir a disponibilidade e a integridade dos dados.
- **Gestão de Capacidade e Eficiência Operacional:** Planejamento e controle da capacidade tecnológica, análise preditiva de consumo, projeção de crescimento de carga e adequação racional dos recursos.

5.1.2. **Segurança da Informação e Conformidade Técnica** - Essas ações visam fortalecer o núcleo de confiança digital da Instituição, preservando a integridade, a confidencialidade e a autenticidade dos serviços, por meio de:

- **Proteção Ativa:** Implementação e gestão de medidas de segurança (e.g., firewall, antivírus, criptografia), controle de acesso e políticas de segurança, a fim de mitigar riscos e garantir a integridade e confidencialidade das informações.
- **Gestão de Acessos e Rastreabilidade:** Controle de acessos, credenciais e autenticação, com segregação de funções e rastreabilidade de operações.
- **Monitoramento e Resposta a Incidentes:** Tratamento estruturado, registro de evidências e pronta resposta a incidentes de segurança.
- **Gestão de Risco e Auditoria:** Controle de vulnerabilidades, auditoria técnica e manutenção da conformidade com políticas de segurança e normas aplicáveis (e.g., LGPD).

5.1.3. **Monitoramento, Observabilidade e Inteligência Operacional (AIOps)** - A contratação deverá incorporar um novo padrão de observabilidade inteligente e gestão preditiva, transformando a operação tecnológica em uma estrutura autônoma, responsiva e orientada a resultados, com base nos princípios de AIOps. A solução de monitoramento e suporte proativo de última geração deverá possibilitar uma visão integrada e cognitiva (full-stack), mediante:

- **Coleta e Correlação Inteligente:** Coleta contínua de métricas de desempenho e disponibilidade, com correlação inteligente de eventos e identificação automática de causas-raiz.
- **Análise Preditiva e Comportamental:** Uso de modelos de inteligência artificial para antecipar falhas e otimizar recursos.
- **Automação de Processos e Resposta:** Uso de tecnologia para automatizar processos e tarefas relacionadas à entrega do serviço, buscando aumentar a eficiência e liberar recursos humanos, incluindo a automação de workflows de resposta e registro estruturado de ações corretivas.
- **Transparência e Gestão:** Geração de dashboards técnicos e executivos para acompanhamento em tempo real dos Níveis Mínimos de Serviço (NMS).
- **Integração de Governança Operacional:** Integração com soluções de gestão de configuração (CMDB), central de serviços (ITSM) e segurança (SIEM).

5.1.4. **Gerenciamento de Serviços (ITSM) e Governança** - Este conjunto de práticas estabelece um modelo de gestão de serviços e governança digital contínua, garantindo a eficiência, a qualidade e o alinhamento com as necessidades do Órgão:

- **Gestão de Serviços de TI (ITSM):** Para abertura, controle, gerenciamento de demandas, chamados técnicos e tickets de atendimento, deverá ser utilizada a ferramenta de ITSM do Órgão, sendo papel da CONTRATADA realizar as configurações e gerenciamento necessários para o atendimento dos serviços providos.

- **Integração de Sistemas:** Garantir a interoperabilidade e a compatibilidade dos sistemas e aplicações que precisam se integrar de forma eficiente, para a troca de informações e o compartilhamento de dados.
- **Melhoria Contínua e Governança:** Adoção de boas práticas e frameworks reconhecidos, como ITIL v4 e COBIT 2019, para a internalização institucional, padronização e aprimoramento dos processos de TIC.
- **Gestão Baseada em Resultados:** Definição e acompanhamento contínuo dos Indicadores de Níveis de Serviços (INS), com seus Níveis Mínimos de Serviço (NMS), e indicadores de desempenho, com implementação de planos de melhoria contínua.

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

6.1. Além das necessidades de negócio e tecnologias identificadas para a contratação em tela, a escolha da solução deve observar um conjunto de requisitos complementares que garantam a conformidade legal, a sustentabilidade, a segurança em sentido amplo, a gestão eficaz e a adaptabilidade da infraestrutura tecnológica do ITI. Tais requisitos são essenciais para assegurar a perenidade da missão institucional da Autarquia e a otimização do investimento público.

6.2. As demais exigências para a contratação de sustentação de infraestrutura de TIC incluem:

6.2.1. Conformidade Legal e Regulatória:

- O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e a outras legislações aplicáveis.
- Portaria SGD/MGI nº 1.070, de 1º de junho de 2023 (Institui o 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), e suas alterações promovidas pela Portaria SGD/MGI nº 6680, de 4 de outubro de 2024, a Portaria SGD/MGI nº 6.055, de 26 de agosto de 2025 e Portaria SGD/MGI nº 5.921, de 22 de julho de 2026.
- Deve-se garantir a conformidade com as normas específicas da ICP-Brasil, como o DOC-ICP-01 (Declaração de Práticas de Certificação), DOC-ICP-02 (Política de Segurança da ICP-Brasil) e DOC-ICP-05 (Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras).

6.2.2. Sustentabilidade e Boas Práticas Ambientais:

- A solução deve incorporar critérios e práticas de sustentabilidade, observando requisitos de baixo consumo de energia e outros recursos, bem como a logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável.
- A contratada deverá assegurar o cumprimento dos requisitos de sustentabilidade previstos no Guia Nacional de Contratações Sustentáveis, para a seção "Tecnologia da Informação e Comunicação – Aquisição de (ou serviços que utilizem) bens de informática e automação".
- As práticas de sustentabilidade aqui previstas alinham-se ao Plano de Logística Sustentável do ITI, ciclo 2024–2026 (Portaria ITI nº 76/2024), conforme o item 2.8.8.

6.2.3. Minimização da Dependência Tecnológica e Interoperabilidade:

- A Instrução Normativa SGD nº 94/2022, em seu Anexo I, subitem 1.4.1, estabelece diretrizes para evitar a dependência tecnológica e a monopolização de mercado no âmbito da administração pública. Essa preocupação reflete a necessidade de assegurar que as soluções de tecnologia da informação e comunicação (TIC) adotadas nesta contratação sejam sustentáveis, interoperáveis e promotoras de um ambiente competitivo. Nesse contexto, é essencial que a contratação e o desenvolvimento de soluções priorizem padrões abertos e interoperabilidade, promovendo a pluralidade de fornecedores e prevenindo a concentração de mercado em poucos agentes econômicos.
- Atualmente a DITEC/ITI possui soluções de TIC que dão suporte ao atual contrato de sustentação de infraestrutura que poderão ser substituídas em outros processos licitatórios em andamento. Desta forma, busca-se tanto evitar dependência tecnológica e monopolização de mercado, quanto encontrar a solução com melhor custo-benefício que atenda às expectativas e necessidades do órgão. As especificações técnicas desta contratação foram selecionadas, sem prejuízo dos requisitos técnicos e de negócio apresentados.
- Outro aspecto fundamental é a implementação de práticas de governança que garantam a diversificação de fornecedores e evitem a formação de monopólios. As contratações realizadas devem lastreadas por estudos de mercado detalhados e no respeito à competição entre empresas, com utilização de padrões interoperáveis, além de cláusulas contratuais que impeçam a dependência excessiva de um único fornecedor. Essas ações fortalecem o ecossistema tecnológico nacional, ampliam a resiliência das operações públicas e contribuem para a criação de um mercado mais justo e dinâmico.

6.2.4. Necessidade de avaliação prévia do local (vistoria técnica) — requisito decorrente da segurança física exigida pela ICPBrasil

- Os serviços de sustentação recairão sobre a infraestrutura que suporta a Autoridade Certificadora Raiz da ICPBrasil (ACRaiz), a Entidade de Auditoria do Tempo (EAT) e os demais serviços finalísticos do ITI, ambientes submetidos aos requisitos de segurança física mais rigorosos dos normativos da ICPBrasil, em especial a Declaração de Práticas de Certificação da ACRaiz (DOCICP01) e os Requisitos Mínimos para as DPC (DOCICP05).
- Esses ambientes possuem peculiaridades que só podem ser plenamente conhecidas presencialmente, entre as quais: (i) estrutura de acesso segregada em seis níveis de segurança física, com identificação biométrica e cartão eletrônico nas áreas sensíveis; (ii) salacofre blindada (célula estanque em concreto e aço, com proteção eletromagnética), dotada de portas em eclusa e submetida ao princípio do controle duplo — permanência mínima de duas pessoas autorizadas; (iii) módulos de segurança criptográfica (HSM) operados em regime offline, com ativação por controle múltiplo "n de m"; e (iv) sistemas de facilities redundantes (climatização de precisão independente, energia com geradores e nobreaks redundantes, detecção precoce e combate a incêndio por gás inerte, CFTV com guarda de imagens). Tais condições impactam diretamente o tempo de resposta técnica (SLA) e o correto dimensionamento das equipes.
- Por imposição de segurança orgânica, a Política de Segurança da ICPBrasil (DOCICP02) e o DOCICP05 vedam a identificação pública da localização e da topologia dos ambientes da ACRaiz. Assim, o edital não pode detalhar as plantas das salas técnicas, as rotas físicas de dutos e cabeamento segregado e a disposição dos ativos, o que torna a vistoria presencial — realizada sob agendamento restrito e mediante termo de sigilo — o único meio seguro e lícito de franquear ao licitante o conhecimento das condições indispensáveis à elaboração de proposta exequível.
- Somase a isso o regime permanente de fiscalização a que o ambiente está sujeito: auditorias anuais de credenciamento conduzidas pela DAFN e por entidades homologadas (DOCICP08) e auditorias internacionais WebTrust for CA. A não conformidade física ou lógica pode conduzir o ambiente à condição de "inaceitável", com suspensão das operações da ACRaiz — risco de âmbito nacional —, reforçando a necessidade de a contratada conhecer o local in loco.
- Por essas razões, e nos termos do art. 63, §2º, da Lei nº 14.133/2021, a avaliação prévia do local de execução é imprescindível ao conhecimento pleno das condições e peculiaridades do objeto, justificandose a previsão de vistoria técnica prévia no Termo de Referência, assegurados o direito do licitante à sua realização e a possibilidade de substituição por declaração formal (art. 63, §§ 3º e 4º).

6.2.5. Necessidade de estrutura de atendimento local (escritório) no Distrito Federal — requisito de execução decorrente da criticidade e do regime presencial da infraestrutura da ICP-Brasil

- A infraestrutura a ser sustentada está instalada nas dependências do ITI, em Brasília/DF, e opera em regime ininterrupto (24x7x365), com metas de disponibilidade superiores a 99,99% para os serviços finalísticos (AC-Raiz, EAT e Assinaturas Eletrônicas). A continuidade desses serviços é condição da cadeia de confiança da ICP-Brasil, cuja interrupção produz impacto de âmbito nacional.
- Diferentemente de um data center corporativo comum, parte relevante das operações não pode ser executada remotamente: as atividades mais críticas envolvem módulos de segurança criptográfica (HSM) em regime off-line e áreas de acesso físico restrito (sala-cofre com portas em eclusa e princípio do controle duplo, com permanência mínima de duas pessoas autorizadas). Tais condições impõem a presença física de profissionais habilitados para intervenções, testes e resposta a incidentes, sob pena de comprometimento dos Níveis Mínimos de Serviço.
- O tempo de resposta técnica exigido para um ambiente dessa criticidade é incompatível com deslocamentos de longa distância. A manutenção da conformidade permanente perante as auditorias presenciais da DAFN (DOC-ICP-08) e as auditorias internacionais WebTrust — que verificam controles físicos, integridade de CFTV e testes de emergência — pressupõe equipe apta a atuar tempestivamente no local.
- Por essas razões, revela-se imprescindível que a contratada disponha de estrutura administrativa mínima no município de Brasília/DF, apta a assegurar a alocação e a substituição tempestiva dos profissionais e a resposta a incidentes nos prazos pactuados. A exigência não constitui restrição indevida à competitividade: (i) não é condição de habilitação, podendo ser atendida após a assinatura do contrato ("possua ou venha a instalar"), em linha com o Acórdão TCU nº 1176/2021-Plenário; e (ii) é proporcional à essencialidade e ao risco do objeto, sendo indispensável à adequada execução contratual.

6.2.6. Proporcionalidade e motivação das exigências de qualificação técnica e econômico-financeira

- As exigências de habilitação foram dimensionadas de forma proporcional à complexidade, à essencialidade e ao risco do objeto (art. 37, XXI, da Constituição Federal, e art. 70, III, da Lei nº 14.133/2021), evitando restrição indevida à competitividade e observando as diretrizes do art. 67 da mesma Lei.
- Cada exigência de atestado de capacidade técnico-operacional corresponde a um serviço efetivamente previsto no escopo (Apêndice II — Catálogo de Serviços e Apêndice III — Equipes Técnicas) e a ativos existentes no ambiente do ITI (Apêndice I — Infraestrutura de TIC). Os pisos quantitativos foram fixados em patamar não superior a 50% do volume total do parque tecnológico atual, em atenção ao art. 67, § 2º, da Lei nº 14.133/2021, conforme a memória de correspondência a seguir.

Capacidade exigida	Correspondência no ambiente (Apêndice I / escopo)
ITSM e integração de canais	Ferramentas de gestão de serviços (OTRS, GLPI, ServiceNow, Jira SM) — itens 2.4.3 e 2.5.1.
Automação e painéis/observabilidade	Grafana, Prometheus, Zabbix, Opensearch, Graylog — itens 2.4.2, 2.4.5, 2.5.7.
Windows Server + Linux; DNS/DHCP; diretório	Windows (11) e Linux (370); DNS interno/externo (6/6); LDAP (4) — itens 2.5.2, 2.5.6.

SGBD relacionais e não relacionais	PostgreSQL (15), MySQL/MariaDB (8), SQL Server (2), MongoDB — itens 2.4.1 e 2.5.4.
Backup e storage SAN/Fibre Channel	Veeam/Bacula; 4 storages + 7 switches SAN (FC) — itens 2.1.6, 2.5.3.
Antimalware, IPS/NGFW/VPN/WAF	Firewalls (Fortinet 4 + PF 2), IDS/IPS (Suricata/Snort/Wazuh) — itens 2.1.4, 2.5.5.
DevOps/DevSecOps, CI/CD, Kubernetes	Rancher/Docker/Podman/K8s (25), GitLab/Jenkins/ArgoCD — itens 2.2, 2.4.8, 2.5.2.
Balanceamento de carga	F5 BIG-IP, NGINX, HAProxy, MetalLB — item 2.4.6.
Práticas ITIL e NOC 24x7x365	Catálogo de Serviços (Apêndice II) e Equipes Técnicas (Apêndice III); NMS no Apêndice V.

- São adotados, ainda, mecanismos que preservam a competitividade: admite-se o somatório de atestados de contratos executados de forma concomitante e a apresentação em nome da matriz ou de filial, não se impondo limitação de tempo de emissão nem de local de prestação dos serviços, vedadas pelo art. 67, § 2º.
- A qualificação econômico-financeira adota o modelo padronizado da AGU (índices de Liquidez Geral, Liquidez Corrente e Solvência Geral superiores a 1 e, subsidiariamente, patrimônio líquido de 5% do valor anual, aplicável a serviço continuado), sem exigência adicional de capital mínimo ou de garantia de proposta, mostrando-se proporcional à essencialidade e à continuidade do objeto.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A presente sessão contém o registro do quantitativo estimado de serviços necessários para composição da solução que se pretende contratar. Para isso, serão apresentados de forma detalhada os dados históricos e características do ambiente de infraestrutura de TIC da DITEC ITI.

7.2. Como metodologia utilizada para obtenção dessas estimativas, aplicou-se a orientação da Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, mais especificamente no item "10.1. Dimensionamento das necessidades", transcrito abaixo:

“10.1. Dimensionamento das necessidades

10.1.1. O dimensionamento das necessidades é uma etapa fundamental a ser executada durante a construção do Estudo Técnico Preliminar. Para auxiliar essa atividade, a equipe de planejamento pode utilizar informações baseadas no levantamento de ambientes, histórico de chamados, análise de contratos anteriores, previsões constantes no plano anual de contratações, ou ainda informações relacionadas ao padrão esperado de atividades do órgão.”

7.3. Dessa forma, a estimativa da demanda considerou como insumo os levantamentos das informações abaixo:

7.3.1. Análise dos Contratos Administrativos ColaboraGOV/MGI nº 6/2022 e nº 10/2022 firmado com a empresa DSS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO LTDA. Dos quais os detalhes são apresentados adiante neste ETP.

7.3.2. Levantamento da infraestrutura tecnológica da DITEC/ITI, contemplando as informações de ativos, serviços que são providos e tecnologias em uso;

7.3.3. Análise do histórico de demandas realizadas por diversos meio como tickets, projetos, e demais solicitações realizadas;

7.3.4. Levantamento dos Ambientes Cibernéticos (sites) do ITI;

7.3.5. Análise crítica da prestação dos serviços técnicos especializados de operação de infraestrutura de TIC, a fim de levantar possíveis oportunidades de melhoria.

7.3.6. Os perfis profissionais e categorias de serviços existentes na Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, que foram compatibilizados para atendimento da necessidade institucional, bem como a experiência necessária, conjunto de atribuições e certificações visando a correta execução e a qualidade dos serviços prestados.

7.4. Análise dos Contratos Administrativos

7.4.1. A análise do contrato vigente tem por objetivo subsidiar os estudos de estimativa dos quantitativo dos serviços que se pretende contratar, assim como orientação do item 10.4 da Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, transcrito abaixo:

“10.4. Análise do Contrato Atual

10.4.1. Caso o órgão possua contrato em execução para a prestação de serviço de operação de infraestrutura e atendimento a usuários de TIC, o mesmo poderá ser contemplado durante o Estudo Técnico Preliminar para análise do histórico de chamados, bem como dos níveis mínimos de serviços, inclusive para balizar o quantitativo de Perfis a ser estimado.”

7.4.2. O Contrato Administrativo nº 6/2022 (SEI/ITI nº 0761441), cujo é "TERMO DE CONTRATO DE FORNECIMENTO DE SOLUÇÃO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO Nº 06/2022, QUE FAZEM ENTRE SI A UNIÃO, POR INTERMÉDIO DA GERÊNCIA REGIONAL DE ADMINISTRAÇÃO DO MINISTÉRIO DA ECONOMIA NOS ESTADOS DE GOIÁS E TOCANTINS - GRA-GO/TO E A EMPRESA LOGIKS CONSULTORIA E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA".

7.4.2.1. A Adesão ao contrato se deu por meio da ORDEM DE SERVIÇO 12804.000806/2026-79 (ColaboraGov) ao programa ColaboraGov do Ministério da Gestão, Inovação e Serviços Públicos (MGI).

7.4.2.2. O pagamento se dá por descentralização orçamentária ao MGI, Processo SEI/ITI nº

7.4.2.3. A demanda é caracterizada como: Descrição: Serviços de apoio em gestão de TI abrangendo as seguintes áreas: apoio na gestão de serviços de infraestrutura, apoio na gestão de serviços/sistemas e apoio na gestão de dados e informações. Serviços de apoio em gestão de negócios de TI abrangendo as seguintes áreas: apoio à governança de TI e gestão de projetos.

7.4.2.4. Prevê a utilização de aproximadamente 6973 horas no período de 01 de maio a 19 de agosto de 2026 nos serviços apresentados na Tabela 7.01.

Tabela 7.01. Tipos de Serviço na OS ColaboraGov

Conforme catálogo de Serviços Contratação ColaboraGov/MGI (25354392)
2.2. Apoiar na elaboração relatório de acompanhamento de atividades realizadas no período por projeto;
2.5. Repasse de conhecimento da metodologia de Gestão de Projetos;
2.8. Apoiar a avaliação de cenários para interoperação ou integração de informações;
2.10. Análise de requisitos.
3.11. Apoiar a CONTRATANTE na implementação das ações (plano de ação) que visam a alcançar a maturidade de TIC desejada e atender às recomendações e determinações dos Órgãos de Controle Interno e Externo;
5.6. Gerir os níveis de serviços de infraestrutura de TIC;
5.7. Gerir o atendimento aos usuários de serviços de TIC;
5.7. Gerir o atendimento aos usuários de serviços de TIC;
5.10. Apoiar a operação/manutenção dos processos correlatos à gerência de configuração e mudanças, como por exemplo: estruturar o ambiente de configuração, gerar as entregas de artefatos, dentre outros;
5.10. Apoiar a operação/manutenção dos processos correlatos à gerência de configuração e mudanças, como por exemplo: estruturar o ambiente de configuração, gerar as entregas de artefatos, dentre outros;
5.11. Análise e implementação de soluções para monitoramento da infraestrutura fornecida pelo cliente da aplicação e seus respectivos parques de serviços de infraestrutura;
5.19. Prospectar solução de gestão de configuração e mudanças;
6.10. Apoiar a área de negócio nas atividades de testes de aceitação (homologação) de sistemas.
6.13. Projetar a intervenção adaptativa e evolutiva nos componentes de softwares necessários à publicação e disponibilização de releases ou novas aplicações em produção.
6.12. Planejamento da implantação dos componentes de software em ambiente adequado para provimento de release ou novas versões a serem lançadas.
6.14. Atualização ou desenvolvimento de documentação dos componentes de software.
10.1. Propor identidades visuais para sistemas internos, front-ends e de ambientes para páginas web (internet, intranet e blog);
10.2. Validar aderência dos produtos de software à identidade visual da CONTRATANTE;
10.4. Tratamento e criação de imagens gerais para sistemas, sítios, manuais e outros a serem utilizados no ambiente tecnológico da CONTRATANTE.

- 11.6. Apoiar na análise de impacto ao negócio sob todos os riscos levantados, utilizando metodologia aprovada pela CONTRATANTE;
- 11.7. Apoiar a CONTRATANTE na gestão de continuidade do negócio;
- 11.9. Apoiar a CONTRATANTE no tratamento de incidentes, problemas e crises de segurança da informação;
- 11.12. Apoiar a CONTRATANTE com o desenvolvimento de software seguro;
- 11.11. Apoiar a CONTRATANTE na gestão de mudanças nos aspectos relativos à SIC;
- 11.13. Apoiar a CONTRATANTE na auditoria de conformidade referente à SIC.

7.4.3. Há também o Contrato Administrativo nº 10/2022, firmado com a empresa DSS SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO LTDA, que tem como objetivo prover 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), para atendimento das necessidades no âmbito da DITEC/ITI.

7.4.3.1. O modelo de contratação é baseado no valor fixo mensal associado ao cumprimento de níveis de serviços e critérios de qualidade. Os atendimentos são do tipo remoto e são segmentado em Gerenciamento, Infraestrutura e Segurança.

Tabela 7.02. Áreas de Prestação de Serviço do Contrato nº 10/2022

Item	Descrição do Serviço	Unidade de medida
1	GERENCIAMENTO	Unidade/mês
2	INFRAESTRUTURA	Unidade/mês
3	SEGURANÇA	Unidade/mês

7.4.3.2. De acordo com o "Extrato Instrumento de Cobrança NF nº. 13.133 - Março de 2026" (SEI nº 0787852) foi pago e empresa DSS o valor de R\$ 120.184,49 (cento e vinte mil e cento e oitenta e quatro reais e quarenta e nove centavos) referente ao mês de março de 2026.

7.4.3.3. O serviço de Assinatura Eletrônica Avançada no contexto do Instituto Nacional de Tecnologia da Informação (ITI) e do Governo Federal é um dos três tipos de assinaturas eletrônicas previstas na Lei nº 14.063/2020, que estabelece regras sobre o uso dessas tecnologias em interações com órgãos públicos.

7.4.3.4. A atuação da AVANÇADA, neste contexto, não é um serviço único do ITI, mas sim um nível de segurança e validade jurídica regulamentado pelo ITI e implementado pelo Governo Federal.

7.4.3.5. Diante disso os profissionais da DSS realizam serviços voltados para a “AVANÇADA” como:

- Diagnosticar e solucionar problemas técnicos que impedem a conclusão da assinatura em sistemas integrados (ex: erros de comunicação com a API do ITI/Gov.br, incompatibilidade de navegadores, problemas de formato de arquivo);
- Monitoramento 24/7 a conexão e o desempenho da interface de programação de aplicações (API) que comunica o sistema da organização com o serviço de Assinatura Eletrônica Avançada (Gov.br);
- Identificar e relatar imediatamente falhas de comunicação ou lentidão;
- Garantir a manutenção de logs de assinatura (registros de quem, quando e o que foi assinado), que são cruciais para a validade jurídica e rastreabilidade dos documentos.
- Serviço de Security Manager Center do ambiente tecnológico da Avançada;
- Serviços de Proteção perimetral do ambiente tecnológico;
- Sustentação de todos os servidores físicos e virtuais;
- Serviço de proteção de dados utilizando ferramentas de mercado;
- Serviços de redes e conectividades de ambos os sites - Brasília / Rio de Janeiro;
- Sustentação na base de dados dos servidores do órgão;

7.4.3.6. O contrato atual da DSS transforma as exigências legais e a tecnologia do ITI em um serviço operacional contínuo e seguro para a organização contratante.

7.4.4. Após análise realizada na seção 7.4.3 é possível inferir que, para os contratos atualmente vigentes relativos à sustentação de TIC para atender aos serviços que são providos pelo ITI, apresentamos valores que constam na Tabela 07.03 a seguir.

Tabela 7.03. Valor mensal dos contratos vigentes

Contrato Administrativo	Valor referente a um (1) mês
Contrato nº 6/2022 (ColaboraGov) (OS ITI)	R\$ 190.192,00
Contrato nº 10/2022	R\$ 120.184,49
Total	R\$ 310.376,49

7.4.5. Dada a reorganização institucional em curso, a pretensa contratação visa suprir as demandas de serviços e projetos que hoje são atendidas pelas unidades organizacionais do ITI. De forma a recompor o quadro de colaboradores para um número suficiente e adequado.

7.4.6. Esta necessidade se configura a partir do entendimento que a infraestrutura tecnológica e, conseqüentemente, os serviços de TI estão em constante evolução e numa curva crescente de demandas.

7.5. Análise do histórico de demandas

7.5.1. O levantamento do histórico de chamados é um pressuposto para a aplicação do modelo de contratação. A Equipe de Planejamento da Contratação (EPC) realizou um levantamento detalhado de demandas cotidianas e excepcionais, analisando registros do Sistema OTRS, Requisições de Mudança e projetos.

7.5.2. A Equipe de Planejamento da Contratação realizou um levantamento detalhado sobre demandas cotidiana e excepcionais referentes aos Serviços Negociais apresentados no "Apêndice II - Catálogo de Serviços" (SEI/ITI nº 0810873).

7.5.2. Assim, foram analisados registros do Sistema ORTS, Requisições de Mudança e projetos em desenvolvimento

7.5.3. Quantitativos Totais de Chamados da DITEC

7.5.3.1. A análise histórica da ferramenta OTRS da DITEC para o período coberto pelo contrato nº 10/2022 demonstrou um volume total de 113.509 tickets. O foco da demanda está concentrado em sustentação de ambientes e segurança de alto impacto:

Tabela 7.04. Filas Identificadas e Volume no ITSM atual

Fila de Atendimento (Categoria Técnica)	Volume de Tickets (Total)	Foco no Negócio
Infraestrutura (Geral)::Sistemas Operacionais	49.191	Sustentação de Aplicações/Operação de Infraestrutura
Segurança (Geral)::SIEM	9.596	Cibersegurança / Monitoramento de Serviços de TI
Segurança (Geral)::Backup::Veeam	9.170	Armazenamento e Backup
Infraestrutura (Geral)::Redes	3.195	Conectividade e Comunicação

7.5.3.2. Detalhamento Qualitativo dos Chamados Críticos / ICP-Brasil: A natureza dos incidentes mais críticos na infraestrutura que suporta a AC-Raiz, destacando a necessidade de serviços ininterruptos em regime 24x7.

- I. **Sustentação de Aplicações/Sistemas Críticos:** Demandas relacionadas à validade da LCR (Lista de Certificados Revogados) em diferentes sites (RNP, INFOVIA, CONTINGÊNCIA), e problemas de Certificado Site Polícas. Tais problemas são vitais para a operação da ICP-Brasil.
- II. **Backup e Armazenamento:** Incidentes frequentes envolvendo o sistema BACULA (BACULA_FDISK, BACULA_CFTV, BACULA_INTRANET), demonstrando a necessidade de monitoramento e sustentação contínua de rotinas de cópia e recuperação de dados.
- III. **Monitoramento e Segurança Física/Lógica:** Alertas de indisponibilidade de ativos críticos (PING, HTTP) em clusters e switches na SCRJ (incluindo o Cluster SCRJ HOST 34 e Switches Servidores SCRJ), bem como problemas em climatizadores (MINI_MATE, HPM_S20).
- IV. **Cibersegurança e Conformidade:** Demandas para Liberação de regras no firewall, Tratamento dos registros de acesso, e atividades de atualização de keystore, confirmando o foco da contratação em Cibersegurança.

7.5.3.3. Natureza dos Chamados (Operação e Conformidade Crítica) - O histórico demonstra que a maior parte dos tickets está diretamente relacionada à sustentação de serviços essenciais e à conformidade com os normativos da ICP-Brasil (DOC-ICP):

Tabela 7.05. Análise das Filas Identificadas

Categoria da Fila OTRS	Exemplos de Demandas Registradas	Categoria Correlata Portaria 1070/2023
Infraestrutura	Problemas de LCR_VALIDADE (Lista de Certificados Revogados), falhas de BACULA (Backup), problemas em servidores de e-mail, e acesso/configuração no CCD.	Operação de Infraestrutura de TIC (Armazenamento e Backup, Sustentação de Aplicações, Sustentação de Banco de Dados, Conectividade).
Segurança	Liberação de regras no firewall, Atualização de keystore, Tratamento dos registros de acesso, e envio de Lista de Biometrias.	Cibersegurança e Monitoramento de Serviços de TI.
Avançada	Demandas relacionadas a deploy de sistemas (Assinador - Produção - Deploy), e acesso a projetos.	Sustentação de Aplicações, Governança de Serviços Negociais DITEC.

7.5.4. Crítica e Ajuste Necessário na Gestão da Demanda

7.5.4.1. Apenas os dados de tickets não representam a demanda real. A utilização de métricas como a UST, evitadas nesta contratação, era inadequada para serviços de suporte contínuo de TI, que não geram resultados ou produtos aferíveis pelo ente público contratante. Muitos tickets são gerados por alertas automatizados do sistema de monitoramento (NOC/SOC), e não por comunicação direta de um usuário. Exemplos são os problemas de validade de LCR, falhas de PING em ativos críticos do CCD, e alertas de backup (BACULA). A contratação visa a implantação e operação do NOC e SOC, confirmando o foco em Monitoramento de Serviços de TIC.

7.5.4.2. Apenas os dados de tickets não representam a demanda real e total de trabalho da DITEC. Isso ocorre devido a vários fatores:

- I. **Dificuldade de Classificação:** Há uma dificuldade histórica em definir o catálogo de serviços e classificar e contabilizar cada ticket. A métrica UST, usada em contratos passados, demonstrou ser ineficiente e complexa para serviços de suporte contínuo de TI.
- II. **Foco Reativo:** Os tickets capturam majoritariamente demandas reativas (incidentes e requisições de correção). Eles não incluem demandas de natureza proativa, como projetos, atividades de Melhoria Contínua e Gerenciamento de Mudanças, que são essenciais para a sustentação de TIC.
- III. **Fragmentação:** A fragmentação contratual anterior resultou em uma baixa visibilidade consolidada e em demandas não registradas formalmente no OTRS, como aquelas advindas de comunicações paralelas (e-mail, reuniões, projetos).

7.5.4.3. A inexistência de série histórica suficientemente consistente e representativa de registros de chamados impediu a utilização de métodos estatísticos tradicionais para projeção da demanda. Para mitigar essa limitação, a Equipe de Planejamento da Contratação (EPC) adotou

abordagem baseada em múltiplas fontes de informação, combinando análise da infraestrutura tecnológica existente, levantamento dos serviços atualmente prestados, avaliação da criticidade dos ativos suportados, características operacionais dos ambientes monitorados e estimativas de atendimento decorrentes dos requisitos de níveis de serviço estabelecidos. Complementarmente, foram considerados parâmetros de mercado, experiências de contratações similares realizadas por órgãos da Administração Pública e a expertise técnica dos servidores responsáveis pela operação e sustentação do ambiente. Essa metodologia permitiu estabelecer um dimensionamento conservador e compatível com a complexidade do ambiente tecnológico a ser suportado, reduzindo os riscos de subdimensionamento ou superdimensionamento da solução contratada.

7.5.4.4. A contratação busca a implantação e operação de sustentação de infraestrutura de TIC com serviços aferidos por parcelas fixas mensais, ajustadas por Níveis de Serviço. De forma a:

- I. **Elevar a Maturidade:** Superar a baixa maturidade em planejamento e gestão contratuais por meio da definição criteriosa do Catálogo de Serviços e NMS.
- II. **Gerenciar o Fluxo:** Exigir que a ferramenta de gerenciamento de serviços de TIC (ITSM) gerencie, de modo individualizado e apartado, os incidentes e as solicitações de mudanças, implementando o fluxo de classificação de chamados.
- III. **Mensuração Abrangente:** O levantamento da demanda real foi complementado por projetos em desenvolvimento (como ações do PDTIC), demandas cotidianas e outros tipos de comunicação (e-mail), além dos tickets provenientes das duas instâncias do OTRS.

7.5.4.5. Garantir que o ITSM (Sistema de Gerenciamento de Serviços de TIC), seja capaz de:

- I. Gerenciar individualmente os Incidentes e as Solicitações de Mudanças.
- II. Implementar o fluxo de classificação de chamados conforme processos formalizados e controlar o prazo de atendimento.
- III. Melhorar a Eficácia: A meta é reduzir o percentual de reaberturas, medido pelo Indicador de Eficácia no Tratamento de Chamados (IETC), cuja meta é IETC >= 99%.

7.5.4.6. A EPC, ainda, identificou o “Risco 8 – Inexistência de informações históricas do órgão, relativas à prestação de serviços de suporte à infraestrutura”, com impacto de sub ou superdimensionamento contratual.

7.5.5. Relacionamento entre Perfis Profissionais e Equipes Técnicas (squads)

7.5.5.1. O dimensionamento de perfis profissionais e a estruturação em Equipes Técnicas são etapas fundamentais do planejamento. A definição do tipo de profissional (Júnior, Pleno ou Sênior) depende diretamente da natureza, criticidade e complexidade dos serviços a serem prestados. No contexto do ITI, que opera por exemplo a AC-Raiz e a Assinatura Eletrônica Avançada, ou seja, serviços e infraestrutura crítica, a estimativa considerou a maior parte dos perfis como "plenos" e "seniores", dada a criticidade dos serviços.

7.5.5.2. O dimensionamento dos perfis para a nova contratação considera: (i) o histórico de quantitativo de pessoal dos contratos atual e anteriores; (ii) a natureza e criticidade dos serviços; e (iii) o ajuste de quadro para refletir a nova divisão em categorias.

7.5.5.3. O volume de tickets e a criticidade dos problemas (e.g., falha de LCR, falha de backup) corroboram o uso de perfis Plenos e Seniores, que atuarão para manter o Indicador de Suporte Técnico (IST) dentro da meta (IST <= 0,10), e o Indicador de Eficácia no Tratamento de Chamados (IETC) elevado (redução de reaberturas).

7.6. Infraestrutura de Tecnologia da Informação e Comunicação

7.6.1. A Equipe de Planejamento da Contratação realizou um levantamento detalhado da Infraestrutura de Tecnologia da Informação e Comunicação atual, abrangendo descrições e quantitativos de equipamentos, tecnologias, modelos, fabricantes e versões de softwares que compõem a infraestrutura. Além disso, foram identificados o número de usuários e os sistemas utilizados pelo Órgão. A descrição completa desses dados está disponível no "Apêndice I - Infraestrutura de TIC" (SEI/ITI nº 0810756)".

7.6.2. Definição do Local de Prestação dos Serviços

Tabela 7.06. Ambientes Cibernéticos/sítios do ITI

Referência	Descrição	Endereço	Tipo de Atendimento
CCD	Centro de Certificação Digital (CCD) do ITI	(Endereço a ser informado no ato da contratação sob termo de sigilo). Brasília - DF.	Presencial e Remoto

Sede	Sede do Instituto Nacional de Tecnologia da Informação (ITI)	SAUS Quadra 06. Complexo-sede da Anatel, Bloco E, 8º Andar. Brasília - DF. CEP: 70070-940.	Presencial e Remoto
Contingência	Site de Contingência da DITEC/ITI	(Endereço a ser informado no ato da contratação sob termo de sigilo). Rio de Janeiro - RJ.	Remoto

7.6.3. A coordenação das atividades presenciais e das áreas especializadas de TIC será realizada a partir das dependências da sede do ITI.

7.6.4. Todos os deslocamentos das equipes, entre os locais de prestação de serviços definidos, que se fizerem necessários para o desenvolvimento das atividades contratadas serão de responsabilidade da CONTRATADA, através de meios que lhe convir.

7.6.5. Os horários de funcionamento dos ambientes cibernéticos/sítios da CONTRATANTE são de segunda a sexta-feira, entre 07:00 horas e 19:00 horas. De forma que a carga-horária diária do profissional deve estar dentro neste período.

7.6.6. É facultado, nos casos em que houver viabilidade, que a CONTRATADA execute remotamente as suas atividades previstas para execução presencial, desde que o acesso remoto seja realizado de acordo com normas e procedimentos estabelecidos e com ferramentas homologadas pela CONTRATADA. Em todas as circunstâncias deverão ser observados os Níveis Mínimos de Serviço (NMS).

7.7. A Pretensa Contratação

7.7.1. As demandas tecnológicas atuais e futuras da Instituição exigem a adoção de um modelo de sustentação e operação de TI mais dinâmico, resiliente e inteligente, capaz de responder proativamente às novas exigências de disponibilidade, escalabilidade e segurança.

7.7.2. A nova contratação tem como objetivo estratégico assegurar a operação plena e a melhoria contínua das capacidades tecnológicas institucionais, eliminando fragmentações contratuais e adotando como princípios centrais a Integração Operacional, a Gestão Baseada em Resultados (NMS), a Automação Inteligente e a Transparência.

7.8. Perfis Profissionais

7.8.1. Equipes Técnicas

- 7.8.1.1. A Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, ANEXO I, seção 2.3.2, define os serviços em categorias:
- 7.8.1.2. De forma a alinhar as categorias de serviços, seus grupos e os próprios serviços ao cotidiano gerencial, foram definidas as seguintes Equipes Técnicas (squads):
- I. Governança de Serviços de TIC
 - II. Operação de datacenter
 - III. Sustentação de aplicações e banco de dados
 - IV. Infraestrutura de redes e conectividade
 - V. Cibersegurança
 - VI. Gerenciamento e execução de serviços negociais DITEC
 - VII. Gerenciamento e execução de serviços negociais DAFN
- 7.8.1.3. Com o objetivo de garantir a prestação eficiente dos serviços, alinhada às necessidades do Órgão, foi proposto um fluxo de gestão das Equipes Técnicas (ou *squads*) relacionando-as com as categorias de serviços. De forma a prover responsáveis pela interface entre a CONTRATADA e o CONTRATANTE, as Coordenações com responsabilidade regimental pela sustentação dos serviços e pela gestão da infraestrutura de TIC foram organizadas conforme o Tabela 7.07 a seguir:

Tabela 7.07. Relação Equipes Técnicas e Unidades Organizacionais

Equipe Técnica (squad)	Unidade Organizacional
Governança de Serviços de TIC	Diretoria de Infraestrutura Tecnológica (DITEC)
Operação de datacenter	Coordenação-geral de Infraestrutura e Segurança (CGISE) / Diretoria de Infraestrutura Tecnológica (DITEC)

Sustentação de aplicações e banco de dados	Coordenação-geral de Infraestrutura e Segurança (CGISE) / Diretoria de Infraestrutura Tecnológica (DITEC)
Infraestrutura de redes e conectividade	Coordenação-geral de Infraestrutura e Segurança (CGISE) / Diretoria de Infraestrutura Tecnológica (DITEC)
Cibersegurança	Coordenação-geral de Infraestrutura e Segurança (CGISE) / Diretoria de Infraestrutura Tecnológica (DITEC)
Gerenciamento e execução de serviços comerciais DITEC	Coordenação-geral de Operações (CGOPE) / Diretoria de Infraestrutura Tecnológica (DITEC)
Gerenciamento e execução de serviços comerciais DAFN	Diretoria de Auditoria, Fiscalização e Normatização (DAFN)

7.8.2. A partir do levantamento dos profissionais existentes no contrato vigente, do volume de serviços e da infraestrutura de TIC, visando a melhoria da qualidade do serviço prestado, e com base nos perfis existentes na Portaria SGD/MGI nº 1.070, de 1º de junho de 2023.

7.8.3. Requisitos de Experiência Mínima por Senioridade

7.8.3.1. Os requisitos de experiência são padronizados e vinculados à senioridade dos perfis profissionais de referência (Júnior, Pleno e Sênior), conforme Portaria SGD/MGI nº 6.055, de 26 de agosto de 2025:

“7. Os requisitos de experiência profissional de cada Perfil devem estar descritos no Termo de Referência observando as alíneas "f" e "g" do inciso II do art. 16 da Instrução Normativa SGD/ME nº 94, de 2022, e as seguintes diretrizes:

- a) os perfis profissionais com senioridade Junior devem possuir ao menos 1 (um) ano de experiência desempenhando as atividades do respectivo perfil profissional;
- b) os perfis profissionais com senioridade Pleno devem possuir ao menos 3 (três) anos de experiência desempenhando as atividades do respectivo perfil profissional; e
- c) os perfis profissionais com senioridade Sênior devem possuir ao menos 5 (cinco) anos de experiência desempenhando as atividades do respectivo perfil profissional.”

7.8.3.2. A senioridade definida para cada perfil profissional foi definida no "Apêndice III - Equipes Técnicas" (SEI/ITI nº 0810874).

7.8.4. Definição de Senioridade, Regime e Quantidade

7.8.4.1. A partir da identificação dos perfis e do conhecimento dos requisitos de senioridade, foi elaborado o "Apêndice III - Equipes Técnicas" onde as equipes técnicas, perfis profissionais desejados para esta contratação, com base nas necessidades institucionais. Definido regime, janela padrão, carga-horária e perfis profissionais.

7.8.4.2. o Apêndice III - Equipes Técnicas" estabelece relação entre Categorias de Serviço, Perfis Profissionais e outras informações, para a execução dos serviços de Sustentação da Infraestrutura de TIC.

7.8.4.3. A alteração no quantitativo de perfis está diretamente relacionada à necessidade de aprimorar os serviços de segurança da informação e TIC do Órgão, à absorção de tarefas atualmente realizadas pelo serviço de SOC (*Security Operations Center*) e à criação das Equipes Técnicas, incluindo novas áreas de atuação como Suporte Técnico a serviços Comerciais. Sendo essas mudanças são essenciais para atender adequadamente às necessidades apresentadas.

7.8.4.4. Em relação ao contrato atual, além dos ajustes nos perfis, o estudo conduzido pela Equipe de Planejamento da Contratação evidenciou a necessidade de atualizar a equipe estimada, considerando mudanças já ocorridas e as planejadas na infraestrutura de TIC do Órgão.

7.8.4.5. Além disso, observa-se no contrato vigente a necessidade de reorganizar a distribuição dos profissionais entre as áreas de atuação, visando maior eficiência e alinhamento aos fluxos de processos existentes no Órgão. Por essa razão, os perfis foram redistribuídos conforme as demandas identificadas e os fatores estratégicos de cada categoria de serviço.

7.8.4.6. A estimativa considerou a maior parte dos perfis como "plenos" e "seniores", tendo em vista o provimento de serviços e sistemas críticos para a população brasileira, necessitando da atuação de profissionais com a qualificação adequada para sustentar a infraestrutura de TIC.

7.8.5. Dimensionamento e Projeção da Demanda Futura

7.8.5.1. Para a definição do prazo inicial da contratação a Portaria SGD/MGI nº 1.070/2023 define:

"9.3.1. Conforme previsto na Orientação Normativa nº 38, de 13 de dezembro de 2011, da Advocacia-Geral da União, em regra o prazo de vigência é de até 12 meses, entretanto admite-se período superior em função da complexidade e peculiaridade do objeto, conforme trecho a seguir:

Nos contratos de prestação de serviços de natureza continuada deve-se observar que:

- a) O prazo de vigência originário, de regra, é de até 12 meses;
- b) Excepcionalmente, este prazo poderá ser fixado por período superior a 12 meses nos casos em que, diante da peculiaridade e /ou complexidade do objeto, fique tecnicamente demonstrado o benefício advindo para a administração; e
- c) É juridicamente possível a prorrogação do contrato por prazo diverso do contratado originariamente.

9.3.2. O "Guia de boas práticas em contratação de soluções de tecnologia da informação" versão 1.0, do TCU, na página 148, também trata deste aspecto:

6) Em alguns contratos, o custo para a inserção da empresa no órgão pode ser alto (e.g. contratação de service desk), de modo que, se o período de vigência do contrato for curto, a empresa pode considerar que o risco de não haver prorrogação seja alto, o que tende a aumentar os preços ofertados. Em casos desse tipo, é aconselhável definir um período de vigência mais longo (e.g. dois ou três anos), bem como possibilidade de prorrogações (e.g. anuais)."

7.8.5.2. Assim, dada a natureza, criticidade e características institucionais dos ambiente tecnológicos em questão e do ITI, optou-se por prosseguir com a contratação inicial de vinte e quatro (24) meses).

7.8.5.3. O dimensionamento da equipe é fundamental para a estimativa do preço de referência da contratação.

Tabela 7.08. Relação entre Itens da pretensa contratação e Esquipes Técnicas

ITEM	DESCRIÇÃO	Equipes Técnicas (squads)
1	Serviços técnicos especializados de sustentação de infraestrutura crítica de TI	Governança de Serviços de TIC
		Operação de datacenter
		Sustentação de aplicações e banco de dados
		Infraestrutura de redes e conectividade
		Cibersegurança
		Gerenciamento e execução de serviços comerciais DITEC
		Gerenciamento e execução de serviços comerciais DAFN

7.8.5.3. Os itens previstos, em grupo único, para a pretensa contratação são apresentados a seguir.

Tabela 7.09. Informações sobre o itens da pretensa contratação

--	--	--	--	--	--

ITEM	DESCRIÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE
1	Serviços técnicos especializados de sustentação de infraestrutura crítica de TI	27014	Unidade Mensal	24

8. Levantamento de soluções

8.1. De acordo com a portaria SGD/MGI ° 1070, de 1º de junho de 2023, que 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, foi definido que o serviço deve ser contratado por meio do modelo de pagamento fixo mensal, conforme transcrição abaixo do Art 2º:

“Art. 2º A contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação deverá ser realizada por meio de modelo de pagamento fixo mensal, vinculada ao atendimento de níveis mínimos de serviços previamente estabelecidos, conforme quantidades e perfis profissionais mínimos previstos em ordens de serviços.”

8.2. Além disso, conforme consta no artigo 3º da portaria SGD/MGI ° 1070, o modelo estabelecido é de utilização obrigatória:

“Art. 3º O modelo de contratação descrito no Anexo I desta Portaria é de utilização obrigatória para a contratação de serviços de operação de infraestrutura e atendimento a usuários de tecnologia da informação e comunicação.”

8.3. Com base no item nº 1.4, Anexo I, da Portaria nº SGD/MGI nº 1.070, de 1º de junho de 2023, a equipe de planejamento da contratação, levantou alternativas de cenários possíveis para a contratação e realizou de forma criteriosa uma análise de viabilidade:

“1.4. De forma excepcional, admite-se a utilização de outros modelos para a contratação de serviços técnicos especializados de operação de infraestrutura e atendimento a usuários de TIC, desde que solicitado via ofício e obtida a autorização prévia da SGD. Deve-se observar as seguintes orientações:

- a) avaliar a viabilidade de utilização de modelos já adotados na Administração, pois aumenta o nível de padronização nas contratações no âmbito do SISP;
- b) não utilizar métrica de remuneração cuja medição não seja passível de verificação, nos termos da Súmula TCU 269;
- c) avaliar a economicidade dos preços estimados e contratados, realizando a análise crítica da composição de preços unitários e do custo total estimado da contratação; e
- d) abster-se de criar unidades de medida de forma unilateral, sem a avaliação técnica, econômica e de padronização.”

8.4. Os cenários identificados para a contratação pretendida estão dispostos conforme Tabela 8.01 a seguir e a análise de cada um deles nos itens seguintes.

Tabela 8.01. Cenários Identificados

ID	Descrição do Cenário
1	Força de Trabalho Própria do Órgão
2	Contratação por valor fixo mensal
3	Contratação Direta das Empresas Públicas de TIC

8.5. A Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, estabelece no Art. 11, inc. II, que para análise comparativa de soluções, devem ser considerados, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação, observado:

- “... a) necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas;
- b) as alternativas do mercado;

- c) a existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações;
- d) as políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis;
- e) as necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual;
- f) os diferentes modelos de prestação do serviço;
- g) os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;
- h) a possibilidade de aquisição na forma de bens ou contratação como serviço;
- i) a ampliação ou substituição da solução implantada; e
- j) as diferentes métricas de prestação do serviço e de pagamento; ...”

8.6. Nesse sentido, para composição desse estudo técnico, foi realizado a análise dos cenários possíveis para a realização da contratação ora pretendida, como forma de evidenciar as diferentes formas de prestação de serviços e escolha de solução mais vantajosa.

8.7. Necessidades similares em outros Órgãos ou entidades da Administração Pública e as soluções adotadas

8.7.1. Foram identificados, na Tabela 8.02, os projetos recentes para a contratação de serviços técnicos especializados de operação de infraestrutura e atendimento a usuários de TIC realizados por Órgãos Públicos na Administração Pública.

Tabela 8.02. Cenários Identificados

ÓRGÃO	PREGÃO	OBJETO	SOLUÇÃO ADOTADA
INCRA	90005 /2025	Prestação de serviços técnicos especializados de atendimento aos usuários em 1º (primeiro), 2º (segundo) e 3º (terceiro) níveis, com o objetivo de fornecer Sustentação Operacional e Gerenciamento da Infraestrutura de Tecnologia da Informação do INCRA, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos	Contratação por valor fixo mensal
DEFENSORIA PUBLICA DA UNIÃO	90023 /2025	Contratação de empresa especializada de serviços técnicos, orquestração e gestão inteligente redundante, sustentação, suporte e administração de ambiente de infraestrutura de TI da DPU, pelo prazo de 60 (sessenta) meses, renovável por até 120 (cento e vinte) meses, considerando as diretrizes da Instrução Normativa SGD/ME nº 94/2022 e a Portaria SGD/MGI Nº 6.680/2024, conforme condições e exigências estabelecidas no Edital e seus Anexos.	Contratação por valor fixo mensal
TRIBUNAL REGIONAL ELEITORAL DO GOIÁS	90005 /2025	PRESTAÇÃO DE SERVIÇOS CONTÍNUOS DE TÉCNICOS ESPECIALIZADOS EM OPERAÇÃO DE INFRAESTRUTURA, SUSTENTAÇÃO E ATENDIMENTO AO USUÁRIO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, ENGLOBALANDO ATENDIMENTO NA CENTRAL DE SERVIÇOS (SERVICE DESK), SUPORTE TÉCNICO A USUÁRIOS (1º, 2º E 3º NÍVEIS), SUSTENTAÇÃO DE APLICAÇÕES E DE INFRAESTRUTURA DE TIC E SUPORTE ÀS EQUIPES DE GESTÃO DE INFRAESTRUTURA TECNOLÓGICA, PARA O TRIBUNAL REGIONAL ELEITORAL DE GOIÁS	Contratação por valor fixo mensal
INSTITUTO DE PESQUISA ECONOMICA		COMPREENDENDO OPERAÇÃO DE INFRAESTRUTURA E ATENDIMENTO AOS USUÁRIOS DE TIC, COM UTILIZAÇÃO DE CENTRAL DE ATENDIMENTO REMOTO E/OU PRESENCIAL, A CRITÉRIO DO CONTRATANTE, CONTEMPLANDO OPERAÇÕES DE SUPORTE, SUSTENTAÇÃO E MANUTENÇÃO DOS SERVIÇOS E DA INFRAESTRUTURA	

APLICADA - IPEA	90043 /2025	EXISTENTE E A EXECUÇÃO DE TAREFAS DE DEMANDA NÃO ROTINEIRAS, MEDIANTE PAGAMENTO DE VALOR FIXO MENSAL ASSOCIADO A ATENDIMENTO DE NÍVEIS MÍNIMOS DE SERVIÇO (NMS), CONFORME CONDIÇÕES E EXIGÊNCIAS ESTABELECIDAS NO TERMO DE REFERÊNCIA.	Contratação por valor fixo mensal
-----------------	-------------	--	-----------------------------------

8.8. Alternativa de mercado

8.8.1. Existem diversas empresas no mercado que prestam os serviços técnicos especializados de operação de infraestrutura e atendimento a usuários de TIC com várias possibilidades, principalmente nas modalidades indicadas no levantamento de soluções.

8.8.2. Nos projetos recentes para a contratação de serviços técnicos especializados de operação de infraestrutura e atendimento a usuários de TIC realizados por Órgãos Públicos na Administração Pública, as seguintes empresas foram vencedoras do processo licitatório.

Tabela 8.03. Licitantes vencedoras dos Pregões Listados

Órgão	Pregão	Empresa Vencedora
INCRA	90004 /2025	POSITIVO S+ SOLUCOES EM TI S.A
DEFENSORIA PUBLICA DA UNIÃO	90023 /2025	POSITIVO S+ SOLUCOES EM TI S.A
TRIBUNAL REGIONAL ELEITORAL DO GOIÁS	90005 /2025	ILHA SERVICE TECNOLOGIA E SERVICOS LTDA
INSTITUTO DE PESQUISA ECONOMICA APLICADA - IPEA	90043 /2025	TECHCOM TECNOLOGIA E INFORMATICA LTDA

8.9. A existência de software público brasileiro, quando aplicável

8.9.1. Por se tratar de contratação de serviços técnicos especializados de operação de infraestrutura e atendimento a usuários de TIC, esse item não se aplica a presente contratação.

8.10. As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ brasil, quando aplicáveis

8.10.1. Por se tratar de contratação de serviços técnicos especializados de operação de infraestrutura e atendimento a usuários de TIC, esse item não se aplica a presente contratação.

8.11. As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual

8.11.1. Para as soluções identificadas, o ITI deverá disponibilizar espaço físico para a contratada e fornecer as estações de trabalho que serão utilizadas pelos funcionários que irão prestar os serviços de forma presencial, caso necessário.

8.12. Os diferentes modelos de prestação do serviço

- I. Cenário 1 - Força de Trabalho Própria do Órgão
- II. Cenário 2 - Contratação por valor fixo mensal
- III. Cenário 3 - Contratação Direta das Empresas Públicas de TIC

8.13. Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes.

8.13.1. Cenário 1 - Força de Trabalho Própria do Órgão:

8.13.1.1. A solução consiste em utilizar-se da própria força de trabalho das áreas de TIC do Instituto Nacional de Tecnologia da Informação (ITI), especificamente da Diretoria de Infraestrutura Tecnológica (DITEC) e outras áreas que possuem profissionais de TI para atendimento das necessidades institucionais.

8.13.1.2. Neste caso, tendo em conta a realidade dos recursos humanos lotados nessas áreas, seria necessário redistribuir a força de trabalho atual para funções relacionadas à execução dos serviços e principalmente reforçar o quantitativo de pessoal, recorrendo a mecanismos de recrutamento com apoio de outras unidades da Administração Pública Federal (APF), tais como:

- Realização de processos seletivos junto à comunidade do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP);
- Realização de concurso público para contratação de novos servidores públicos;
- Recrutamento interno para mobilização de servidores do quadro do Órgão.

8.13.1.3 Para implantação dos serviços nas condições necessárias, e atender satisfatoriamente os requisitos de negócio, seria necessário realizar uma série de ações de curto e médio prazos, algumas das quais independem do controle do ITI:

- Instalação de uma Central de Atendimento no modelo incluindo toda a infraestrutura ITIL, necessária e pessoal capacitado em tecnologia da informação;
- Sustentação, com recursos próprios, de sistema ITSM (Software de Gerenciamento de Serviços), compreendendo atividades de configuração, migração de dados e customização, com dedicação de recursos específicos;
- Aprovação e realização de processos seletivos e/ou convênio para disponibilização de pessoal;
- Capacitação de todo a equipe envolvida, principalmente em conhecimento técnico-operacional.

8.13.2. Cenário 2 - Contratação por valor fixo mensal:

8.13.2.1. Este cenário trata da execução indireta dos serviços nos termos do Decreto nº 9.507/2018 e no modelo de Central de Serviços, por meio da realização de processo licitatório, a exemplo de diversas instituições públicas que já possuem este tipo de contrato, conforme levantamento de contratações similares realizada neste Estudo.

8.13.2.2. A solução deverá atender ao modelo de contratação de serviços de operação de infraestrutura e atendimento ao usuário de TIC, instituída pela Portaria SGD/MGI nº 1070/2023:

"Art. 2º A contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação deverá ser realizada por meio de modelo de pagamento fixo mensal, vinculada ao atendimento de níveis mínimos de serviços previamente estabelecidos, conforme quantidades e perfis profissionais mínimos previstos em ordens de serviços. (Alterado pela Portaria SGD/MGI nº 6.680, de 04 de outubro de 2024)

Parágrafo único. O modelo não se configura como de dedicação exclusiva de mão de obra, contratação por homem/hora e tampouco por postos de trabalho.

Art. 3º O modelo de contratação descrito no Anexo I desta Portaria é de utilização obrigatória para a contratação de serviços de operação de infraestrutura e atendimento a usuários de tecnologia da informação e comunicação."

8.13.2.3. O modelo consiste em permitir que a gestão contratual esteja alinhada com a gestão da qualidade dos serviços prestados, estabelecendo níveis de serviço e indicadores de desempenho mínimos para a execução dos serviços contratados. Assim, os resultados são medidos com base em indicadores vinculados às fórmulas de cálculo específicas, apurados temporalmente e continuamente monitorados, objetivando o cumprimento das metas estabelecidas.

8.13.2.4. Desta forma, a empresa é incentivada a manter o ambiente operacional o mais estável e automatizado possível, a fim de empregar o mínimo de capital humano. O modelo traz vantagem por facilitar a fiscalização dos serviços prestados, avaliando o atendimento dos níveis de serviço e indicadores de desempenho mínimos estabelecidos.

8.13.2.5. Incentiva a melhora da qualidade dos serviços e ambientes de TI de modo que sua estabilidade e performance se reflita na redução de chamados e incidentes, consumindo menos o seu corpo técnico. Desde que mantidos os níveis de serviço, a empresa tende a buscar a eficiência em seus processos e comportamentos dos colaboradores, de modo a manter o ambiente o mais estável possível, podendo manter o mínimo de profissionais no dia a dia.

8.13.2.6. É importante salientar que a definição correta dos níveis de serviço exigidos, bem como o foco na sua fiscalização são os fatores principais de sucesso desse modelo, de modo que o alinhamento desses níveis de serviço às necessidades reais dos usuários deve ser priorizado.

8.13.2.7. Deste modo, equipes de gestão e fiscalização podem concentrar seus esforços nos atendimentos aos níveis de serviço exigidos, em melhorias dos processos e em novos projetos, enquanto a empresa se concentra em melhorar ao máximo a eficiência de seus processos e indicadores de disponibilidade, performance e uso dos recursos de TI.

8.13.3. Cenário 3 - Contratação Direta das Empresas Públicas de TIC:

8.13.3.1. Consiste na contratação direta das empresas públicas de TI para execução dos serviços, com base nas experiências anteriores e modelos vigentes, tendo em vista a legislação específica e natureza estratégica dos serviços.

8.13.3.2. O cenário pressupõe a contratação por meio de dispensa de licitação, lastreada nos seguintes dispositivos:

- Art. 72 da Lei nº 14.133/2021;
- Lei nº 5.615/1970;
- Lei nº 6.125/1974.

8.13.3.3. Este modelo visa não apenas garantir a operação contínua e eficiente da infraestrutura de TI, mas também assegurar que os serviços prestados pela empresa pública de TIC estejam alinhados com as necessidades estratégicas e operacionais do Órgão.

8.13.3.4. A empresa pública de TI geralmente possui uma forte base de conhecimento institucional sobre as necessidades e requisitos específicos do governo ou das entidades públicas. Isso pode resultar em uma melhor compreensão das políticas e das estratégias governamentais, contribuindo para a implementação de soluções de TI mais alinhadas com os objetivos institucionais.

8.13.3.5. Em resumo, o modelo de contratação direta de uma empresa pública de TI visa combinar a flexibilidade e a especialização técnica necessárias para fornecer soluções de TI eficazes e alinhadas aos interesses públicos, ao mesmo tempo em que garante a transparência e a responsabilidade na gestão de recursos públicos.

8.14. A possibilidade de aquisição na forma de bens ou contratação como serviço

8.14.1. A contratação oriunda das soluções indicadas se dará na forma de contratação de serviços.

8.14.2. A possibilidade de aquisição na forma de bens não se aplica à presente contratação.

8.15. A ampliação ou substituição da solução implantada

8.15.1. A presente contratação visa substituir os Contratos Administrativos vigentes citados anteriormente. Dessa forma, não se aplica a possibilidade de ampliação da solução implantada, somente a sua substituição por meio de uma nova contratação, objeto do presente estudo técnico.

8.16. As diferenças métricas de prestação do serviço e de pagamento

8.16.1. No Cenário 1, a Força de Trabalho Própria do Órgão, por se tratar da utilização da própria força de trabalho das áreas de TIC, não se aplica uma métrica de prestação de serviço e de pagamento, havendo nesse caso o custo da folha de pagamento dos Servidores e demais custos administrativos necessários para execução das atividades.

8.16.2. Já no Cenário 2, a contratação por valor fixo mensal, é adotado o modelo de pagamento fixo mensal associado ao atendimento de níveis mínimos de serviço (NMS) e mensurado a partir da estimativa de Categorias de Serviço e seus respectivos Perfis de Trabalho, por meio de Mapa de Pesquisa Salarial de referência, utilização de Fator-K, apoiados por um modelo de Planilha Simplificada para Estimativa do Valor Mensal do Serviços, elaborados e mantidos pelo Órgão Central do SISF.

8.16.3. Para o Cenário 3, Contratação Direta das Empresas Públicas de TIC, o modelo de prestação de serviço e de pagamento adotado costuma ser definido pela Empresa Pública de TIC contratada, dependendo das negociações contratuais e das necessidades específicas de cada Órgão, podendo ser por pagamento fixo, projeto ou por uso, uma vez que fornecem os serviços de forma padronizada e alinhados com as políticas governamentais.

9. Análise comparativa de soluções

9.1. Comparativo de Vantagens e Desvantagens entre os Cenários identificados

9.1.1. Cenário 1 - Força de Trabalho Própria do Órgão: Vantagens e desvantagens.

9.1.1.1. Vantagens:

- a) Uma equipe própria pode estar mais alinhada com os objetivos estratégicos de longo prazo do Órgão e ser mais receptiva a iniciativas de melhoria contínua e inovação tecnológica que agreguem valor à instituição;
- b) Os membros da equipe própria têm um conhecimento profundo das operações, políticas e processos específicos do Órgão. Isso pode facilitar a implementação de soluções de TIC que estejam alinhadas com as necessidades e objetivos da instituição;
- c) Com uma equipe própria, o Órgão pode ter maior controle sobre a priorização de projetos e a gestão de recursos. Isso permite uma maior flexibilidade para adaptar-se a mudanças nas necessidades organizacionais e responder rapidamente a novas demandas.
- d) Embora inicialmente possa parecer mais caro manter uma equipe própria, a longo prazo pode resultar em economias significativas. Isso porque não há necessidade de pagar margens de lucro a empresas terceirizadas e os investimentos em capacitação e desenvolvimento da equipe interna podem ser amortizados ao longo do tempo.

9.1.1.2. Desvantagens:

- a) O ITI não possui, em seu quadro, a quantidade de profissionais de TIC necessários para o atendimento das necessidades levantadas, mesmo com a realização de concurso público para recrutamento de novos Servidores, a capacidade técnica e o local de exercício não estão no controle da DITEC. Acrescenta-se a essa dificuldade o fato de que o Órgão não dispõe de carreiras cuja atividade finalística seja a sustentação técnica de infraestrutura e serviços de TIC, uma vez que por definição tais serviços são tratados como passíveis de execução indireta;
- b) Uma equipe própria pode ser menos flexível em termos de escala e capacidade de resposta rápida a picos de demanda, projetos especiais ou emergências. Isso pode ser especialmente desafiador em situações em que há uma necessidade urgente de recursos humanos adicionais ou conhecimentos técnicos específicos;
- c) Limitações em termos de especialização e experiência em comparação com empresas especializadas de TIC. Problemas complexos ou novas tecnologias podem exigir habilidades específicas que a equipe interna pode não possuir inicialmente, necessitando de mais tempo para desenvolver competências adequadas;
- d) Uma equipe interna pode ter uma visão limitada devido à sua exposição restrita a um único ambiente organizacional. Isso pode resultar em soluções que não aproveitam as melhores práticas ou experiências externas que poderiam ser benéficas para a organização;
- e) A alta rotatividade de Servidores de TIC no Executivo Federal, considerando a baixa atratividade dos cargos em consequência dos baixos salários do Executivo, comparados aos cargos correlatos dos demais poderes, Judiciário e Legislativo, e até mesmo da iniciativa privada.

9.1.2. Cenário 2 - Contratação por valor fixo mensal: Vantagens e desvantagens

9.1.2.1. Vantagens:

- a) Maior facilidade de obtenção do valor médio estimado da contratação, considerando a padronização do Modelo por meio da portaria SGD/MGI nº 1.070, de 1º de junho de 2023, com a composição do preço de referência aplicando o salário dos perfis profissionais publicados pela SGD em conjunto com o fator-k de referência também publicado pela SGD;
- b) A remuneração dos serviços está vinculada a resultados e ao atendimento dos acordos de níveis de serviços - ANS, gerando incentivo na prestação rápida, eficiente e ininterrupta de serviços, que por sua vez, trazem excelência no acesso aos recursos e serviços de rede e sistemas da Administração Pública Federal. Isso confere agilidade e presteza aos processos institucionais que se utilizam de tais serviços;
- c) Não há necessidade de negociação de atividades rotineiras utilizadas para o atendimento aos usuários, como em modelos integralmente com UST, pois as atividades são especificadas pela contratada com o objetivo de manter a disponibilidade e agilidade na prestação dos serviços;
- d) Os indicadores estabelecidos neste modelo de contratação estão conectados com o que é importante e crítico de ser monitorado e avaliado, diminuindo o esforço e melhorando a atenção dos gestores naquilo que é relevante;
- e) Permite que a organização planeje seus gastos com TI de forma previsível. Ao saber exatamente quanto será pago mensalmente, facilita o controle orçamentário e a gestão financeira, eliminando surpresas relacionadas a custos variáveis.

9.1.2.2. Desvantagens:

- a) Este modelo é associado ao ambiente tecnológico atual do órgão e eventuais alterações de grande magnitude podem provocar um desequilíbrio na relação contratual. No entanto, tais desequilíbrios poderiam vir a ser mitigados por meio de aditivos ao contrato;
- b) Pode haver um aumento no esforço administrativo por parte da equipe responsável pela fiscalização do contrato, em razão da necessidade de monitorar a efetiva atuação dos perfis profissionais previstos na Ordem de Serviço, bem como verificar o cumprimento das obrigações trabalhistas por parte da contratada.
- c) Pode ocorrer desequilíbrio contratual, na medida em que não é possível prever a extensão, tamanho e quantidade dos projetos que podem ser demandados ao longo da vigência contratual. A alternativa seria a celebração de aditivos ao contrato.

9.1.3. Cenário 3 - Contratação Direta das Empresas Públicas de TIC: Vantagens e desvantagens

9.1.3.1. Vantagens:

- a) Empresas públicas são orientadas para atender aos interesses públicos e às necessidades específicas das entidades governamentais, garantindo alinhamento com as políticas e diretrizes governamentais;
- b) Como entidades estatais, empresas públicas são geralmente submetidas a regulamentações rigorosas de transparência e prestação de contas. Isso proporciona maior controle sobre a gestão dos recursos públicos e garante uma governança eficaz;
- c) Possuem um conhecimento profundo das políticas, processos e sistemas internos dos órgãos governamentais para os quais prestam serviços. Isso facilita a implementação de soluções de TIC alinhadas com as necessidades específicas da administração pública;

d) Seguem diretrizes rigorosas de segurança da informação e estão mais familiarizadas com as exigências regulatórias e legais específicas do setor público, garantindo a conformidade e a proteção dos dados governamentais;

9.1.3.2. Desvantagens:

a) Empresas públicas podem estar sujeitas a uma maior burocracia e processos internos, o que pode resultar em prazos mais longos para tomada de decisões e implementação de mudanças. Isso pode afetar a agilidade na entrega de serviços e na resolução de problemas.

b) Como entidades públicas, empresas públicas podem enfrentar desafios na competição com fornecedores privados em termos de custos, eficiência e inovação. Isso pode resultar em serviços de TIC que não sejam tão competitivos ou avançados quanto os oferecidos por empresas privadas.

c) Em alguns casos, empresas públicas podem ter uma cultura organizacional menos orientada para a inovação e a adaptação rápida às mudanças tecnológicas. Isso pode resultar em serviços de TIC que não aproveitam plenamente as últimas tecnologias ou práticas de mercado.

d) No geral, o custo dos serviços prestados por empresas públicas de TIC tem um custo elevado comparado às empresas privadas de TIC que prestam os mesmos serviços, muito se deve aos altos salários dos empregados públicos assim como baixa produtividade.

e) Tipicamente, as empresas públicas que prestam serviços de Tecnologia da Informação à Administração Pública Federal (ex. SERPRO, DATAPREV, TELEBRAS) não possuem ofertas puramente de serviços de sustentação de infraestrutura e de serviços do cliente, atuando preferencialmente em modelos onde fornecem a própria infraestrutura e os serviços de forma conjugada.

9.2. Padrões de Governo

9.2.1. Em relação às políticas, aos modelos e aos padrões de Governo, a Tabela 9.01 a seguir expressa as características das soluções analisadas.

Tabela 9.01. Comparativo Padrões de Governo

Requisito	Cenário	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	x		
	2	x		
	3	x		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	1			x
	2			x
	3			x
A Solução é composta por software livre ou software público? (quando se tratar de software)	1			x
	2			x
	3			x

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	1			x
	2			x
	3			x
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			x
	2			x
	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)	1			x
	2			x
	3			x

9.3. Comparativo qualitativo

9.3.1. A Tabela 9.02 a seguir correlaciona os requisitos relacionados ao atendimento das necessidades com cada uma das alternativas de cenários elencados.

Tabela 9.02. Comparativo sob a perspectiva dos requisitos da contratação

Requisitos		Cenário 1	Cenário 2	Cenário 3
Negócio	Aderência à Legislação e Normativos	Sim	Sim	Sim
	Alinhamento Institucional	Sim	Sim	Sim
	Sustentação da Missão Finalística	Sim	Sim	Sim
	Integração e Eficiência Administrativa	Sim	Sim	Sim
	Sustentação e Disponibilidade de Missão Crítica	Sim	Sim	Sim
	Segurança e Conformidade Regulatória	Sim	Sim	Sim
	Continuidade de Negócio e Recuperação	Sim	Sim	Sim

	Gestão Proativa e Observabilidade	Sim	Sim	Sim
Tecnológico	Administração Técnica e Manutenção	Não	Sim	Sim
	Virtualização e Nuvem	Sim	Sim	Sim
	Continuidade e Recuperação de Dados (BCP/DRP)	Sim	Sim	Sim
	Gestão de Capacidade e Eficiência Operacional	Não	Sim	Sim
	Proteção Ativa	Sim	Sim	Sim
	Gestão de Acessos e Rastreabilidade	Sim	Sim	Sim
	Monitoramento e Resposta a Incidentes	Sim	Sim	Sim
	Gestão de Risco e Auditoria	Sim	Sim	Sim
	Coleta e Correlação Inteligente	Não	Sim	Sim
	Análise Preditiva e Comportamental	Não	Sim	Sim
	Automação de Processos e Resposta	Sim	Sim	Sim
	Transparência e Gestão	Sim	Sim	Sim
	Integração de Governança Operacional	Sim	Sim	Sim
	Gestão de Serviços de TI (ITSM)	Sim	Sim	Sim
	Integração de Sistemas	Sim	Sim	Sim
	Melhoria Contínua e Governança	Sim	Sim	Sim
	Gestão Baseada em Resultados	Sim	Sim	Sim
	Conformidade Legal e Regulatória	Sim	Sim	Não

Demais Requisitos	Sustentabilidade e Boas Práticas Ambientais	Sim	Sim	Sim
	Minimização da Dependência Tecnológica e Interoperabilidade	Sim	Sim	Não
Resultado da Análise		Não	Sim	Não

10. Registro de soluções consideradas inviáveis

10.1. Registram-se a seguir as soluções consideradas inviáveis e as respectivas justificativas.

10.1.1. Cenário 1 - Força de Trabalho Própria do Órgão

10.1.1.1. A possibilidade de atendimento da presente demanda por meio de força de trabalho própria não é inexecutável, porém, configura-se inviável, considerando que não é possível atender os requisitos temporais da contratação, imprescindíveis para a manutenção satisfatória dos serviços de TIC oferecidos pelo ITI.

10.1.1.2. A implementação das iniciativas necessárias para a adoção da solução causaria grande impacto na gestão operacional dos ambientes durante o processo necessário à sua efetivação, não havendo como garantir nem esperar que tais ações sejam realizadas em curto prazo. Durante este período, o esforço operacional e de gestão impostos às Áreas de TIC causariam sérios riscos de indisponibilidade e insatisfação dos usuários, bem como de desatendimento das metas estratégicas do Órgão.

10.1.1.3. Ademais, a despeito de não se configurar ilegalidade, o cenário contraria a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, que estabelece que os serviços serão preferencialmente objeto de execução indireta na Administração Pública Federal, em atendimento ao disposto no art. 2º do Decreto nº 9.507, de 21 de setembro de 2018 e ao art. 1º da Portaria MPDG nº 443, de 27 de dezembro de 2018:

“Art. 1º No âmbito da administração pública federal direta, autárquica e fundacional, serão preferencialmente objeto de execução indireta, dentre outros, os seguintes serviços:[...]

XXIII - serviços de tecnologia da informação e prestação de serviços de informação;[...]"

10.1.1.4 Por fim, é importante reforçar que, mesmo que o quadro permanente do ITI possua o conhecimento técnico e a expertise a respeito dos recursos operacionalizados para o necessário provimento dos serviços de TIC, é indubitável que o apoio de pessoal técnico especializado para a execução das atividades rotineiras e operacionais implica em melhores condições para que o corpo permanente de Servidores possa executar atividades de planejamento, supervisão, coordenação e controle dos recursos de Tecnologia da Informação relativos ao funcionamento do respectivo negócio.

10.1.2. Cenário 3 - Contratação Direta das Empresas Públicas de TIC

10.1.2.1. Observa-se dos serviços de tecnologia da informação fornecidos por empresa públicas como o Serviço Federal de Processamento de dados (SERPRO), um movimento em direção à priorização da entrega de soluções estratégicas para o Governo, como infraestrutura e sustentação para sistemas estruturantes (ex: Comprasnet-SIASG, SIAFI e Infraestrutura de Chaves Públicas - Certificação Digital), deixando, preferencialmente, para o mercado privado, a entrega de serviços técnicos especializados de atendimento ao usuário e de operação de infraestrutura de TIC dos Órgãos.

10.1.2.2. Em relação aos normativos vigentes, conforme orienta a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, os serviços técnicos especializados de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação devem ser contratados por meio de processo licitatório:

“21.16. Critérios Técnicos para Seleção do Fornecedor

20.16.1. Considerando as características do objeto, cujos padrões de desempenho e qualidade permitem definições objetivas de serviços com base em especificações usuais de mercado, o processo licitatório deve ser realizado na modalidade Pregão, tipo Menor Preço, na forma eletrônica.”

10.1.2.3. Vale ressaltar que não há impedimento quanto à participação de empresas públicas de TIC em processo licitatório com ampla concorrência segundo as características do mercado.

10.1.2.4. Dessa forma, considerando o atendimento do princípio constitucional da economicidade e o atendimento às necessidades técnicas e de negócio do ITI, este cenário configura-se inviável.

11. Análise comparativa de custos (TCO)

11.1. Considerando que há apenas uma solução viável nos termos da Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, Cenário 2 - Contratação por valor fixo mensal, não se aplica a análise comparativa de custos, em conformidade com o art. 11, inc. III da IN SGD/MGI nº 94/2022.

11.2. Cálculo de Custos Totais de Propriedades (TCO)

11.2.1 Para a estimativa de preços da Contratação por valor fixo mensal (Cenário 2), foi utilizada a Planilha Simplificada para Estimativa do Valor Mensal do Serviços, elaborada e mantida pelo Órgão Central do SISP, de acordo com a Portaria SGD/MGI nº 1.070, de 1º de junho de 2023,e suas alterações, sendo consolidados os valores na Tabela 11.01. a seguir.

Tabela 11.01. Itens da pretensa contratação

ITEM	DESCRIÇÃO	CATSER	UNIDADE DE MEDIDA	Qtde.	MENSAL	12 meses	24 meses
1	Serviços técnicos especializados de sustentação de infraestrutura crítica de TI	27014	Unidade Mensal	24	R\$ 648.289,09	R\$ 7.779.469,08	R\$ 15.558.938,16

* Valores Estimados

11.2.2. Projeção dos Valores Anuais dos Serviços

11.2.2.1. Para registro dos custos totais de propriedade foi considerado a variação do Índice de custo da tecnologia da informação (ICTI), calculado pelo Ipea, acumulado no período de 12 meses, de jun/2025 a mai/2026, de 4,45%. (Fonte: <https://www.ipea.gov.br/cartadeconjuntura/index.php/2025/10/indice-de-custo-da-tecnologia-da-informacao-icti-maio-de-2025/>)

11.2.2.2. Nota Metodológica do Modelo (2026) - demonstração dos procedimentos e métodos adotados na realização de pesquisa de preços para obtenção de mapa de pesquisa salarial e do fator-k limite a serem adotados na estimativa do valor mensal de contratos que utilizam o Modelo de Contratação de Serviços de Operação de Infraestrutura e de Atendimento a Usuários de TIC instituído pela Secretaria de Governo Digital. (Fonte: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/legislacao/modelo-de-contracao-de-servicos-de-operacao-de-infraestrutura-e-de-atendimento-a-usuarios-de-tic/anexos/sei_60048248_nota_tecnica_15961.pdf).

11.2.2.3. Os valores apresentados na Tabela 11.02 tem como base a estimativa de valor realizado por meio da "Planilha Simplificada para Estimativa do Valor" ("Planilha ETP 6/2026 - Apêndice VII - Planilha Simplificada para Estimativa de Valor (SEI/ITI nº 0806101), corrigidos pelo Índice de custo da tecnologia da informação (ICTI).

Tabela 11.02. Estimativa financeira geral para 24 meses

	Ano 01	Ano 02	TOTAL 24 MESES
Valor Estimado sem correção	R\$ 7.779.469,08	R\$ 7.779.469,08	R\$ 15.558.938,16
Correção ICTI (4,45%)	R\$ 0,00	R\$ 346.186,37	R\$ 346.186,37
Valor estimado após correção	R\$ 7.779.469,08	R\$ 8.125.655,45	R\$ 15.905.124,53

11.2.3. Memória de Cálculo

- 11.2.3.1 Para calcular o custo anual total da contratação foi utilizado o mecanismo recomendado pela Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, conforme a seguinte sequência:
- I. Obtiveram-se os respectivos perfis e salários de referência dos profissionais e quantitativos estimados dos mesmos;
 - II. Multiplicou-se os respectivos salários de referência de cada perfil pelo fator K definido na referida Portaria, obtendo-se o valor mensal;
 - III. Para cada quantitativo de perfis definidos, multiplicou-se o custo unitário do perfil pela quantidade estimada, obtendo-se o custo mensal da Equipe Técnica;
 - IV. O somatório dos valores mensais de cada Equipe Técnica resultou no valor mensal estimado para cada item da contratação;
 - V. Multiplicando-se o valor do item anterior por 12 (doze) obteve-se o valor anual estimado da contratação;
 - VI. Para os valores anuais dos anos subsequentes, foi aplicada uma correção de 4,45%, referente ao Índice de Custo da Tecnologia da Informação (ICTI) acumulado nos últimos 12 meses, correspondente ao período de junho de 2025 a maio de 2026.
- 11.2.3.2 Dessa forma, obteve-se o TCO total para os próximos dois anos, conforme apresentado na Tabela 11.03 a seguir.

Tabela 11.03. Custo Total Estimado

Total do Custo projetado	Valores
Valor total da contratação para 24 meses (vigência do contrato) considerando a aplicação do Índice de Custo da Tecnologia da Informação (ICTI) de 4,45%	R\$ 15.905.124,53

11.3. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

- 11.3.1. Considerando que há apenas uma solução viável nos termos da Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, Cenário 2 - Contratação não é se aplica o mapa comparativo dos cálculos totais de propriedade, em conformidade com o art. 11, inc. por valor fixo mensal, III da IN SGD/MGI nº 94 /2022.
- 11.3.2. ITEM 01: Serviços técnicos especializados de sustentação de infraestrutura crítica de TI

Tabela 11.04. Estimativa de Custo Total Estimado das Equipes Técnicas para o ITEM 01

Equipe Técnica	Perfil	Quantidade (B)	Custo unitário mensal do Perfil (C)	Custo total mensal por Perfil (D = C x B)
GOVERNANÇA DE SERVIÇOS DE TIC	Analista de suporte computacional Júnior	2,00	R\$ 8.754,23	R\$ 17.508,47
	Analista de suporte computacional Pleno	1,00	R\$ 11.681,66	R\$ 11.681,66
	Analista de suporte computacional Sênior	1,00	R\$ 17.871,76	R\$ 17.871,76
OPERAÇÃO DE DATACENTER	Analista de suporte computacional Pleno	3,00	R\$ 12.224,99	R\$ 36.674,98
	Analista de suporte computacional Sênior	1,00	R\$ 18.652,56	R\$ 18.652,56
SUSTENTAÇÃO DE APLICAÇÕES E	Administrador de sistemas operacionais Pleno	1,00	R\$ 13.904,46	R\$ 13.904,46
	Administrador de sistemas operacionais Sênior	1,00	R\$ 20.521,74	R\$ 20.521,74
	Analista de sistemas de automação - Pleno	2,00	R\$ 18.466,87	R\$ 36.933,74

BANCO DE DADOS	Administrador de banco de dados - Pleno	1,00	R\$ 14.477,99	R\$ 14.477,99
	Administrador de banco de dados - Sênior	1,00	R\$ 22.447,23	R\$ 22.447,23
INFRAESTRUTURA DE REDES E CONECTIVIDADE	Analista de redes e de comunicação de dados Pleno	1,00	R\$ 15.803,13	R\$ 15.803,13
	Analista de redes e de comunicação de dados Sênior	1,00	R\$ 21.822,50	R\$ 21.822,50
CIBERSEGURANÇA	Administrador em segurança da informação - Júnior	4,00	R\$ 14.981,12	R\$ 59.924,48
	Administrador em segurança da informação - Pleno	4,00	R\$ 20.394,86	R\$ 81.579,44
	Administrador em segurança da informação - Sênior	2,00	R\$ 31.017,47	R\$ 62.034,95
GERENCIAMENTO E EXECUÇÃO DE SERVIÇOS NEGOCIAIS DITEC	Desenvolvedor de sistemas de tecnologia da informação Pleno	1,00	R\$ 22.926,07	R\$ 22.926,07
	Administrador em segurança da informação - Pleno	2,00	R\$ 20.394,86	R\$ 40.789,72
GERENCIAMENTO E EXECUÇÃO DE SERVIÇOS NEGOCIAIS DAFN	Analista de sistemas de automação - Pleno	2,00	R\$ 18.466,87	R\$ 36.933,74
	Administrador de banco de dados - Sênior	1,00	R\$ 22.447,23	R\$ 22.447,23
	Administrador em segurança da informação - Júnior	1,00	R\$ 14.981,12	R\$ 14.981,12
	Administrador em segurança da informação - Pleno	1,00	R\$ 20.394,86	R\$ 20.394,86
		34	Custo Total mensal (F)	R\$ 610.311,81

11.3.2.1. Custo total mensal estimado para horas de sobreaviso das Equipes Técnicas que possuem cobertura de sobreaviso - "OPERAÇÃO DE DATACENTER" e "INFRAESTRUTURA DE REDES E CONECTIVIDADE"

11.3.2.1.1. Foi incluído ao Item 01 o custo total mensal estimado para as horas de sobreaviso das Equipes Técnicas que possuem essa cobertura. O valor desse adicional será calculado com base na média da hora de serviço das equipes com previsão de sobreaviso, levando em consideração a quantidade de profissionais dessas categorias, uma jornada mensal de 176 horas trabalhadas e o fator de sobreaviso de 1/3 da hora normal, conforme a legislação trabalhista vigente.

11.3.2.1.2. Inicialmente, foram relacionadas para o cálculo apenas as equipes técnicas que possuem previsão de sobreaviso, contabilizando as horas de sobreaviso por categoria e o total, além da respectiva quantidade de perfis profissionais e o custo mensal de cada categoria, conforme a Tabela a seguir.

Tabela 11.05. Total de Horas mensais de sobreaviso e custo das Equipes que possuem essa cobertura

Equipe Técnica	Janela Padrão	Horas mensais de Sobreaviso = (22 dias úteis X horas fora da janela padrão, mais 8 dias não úteis x 24 horas)	Quantidade total de perfis por Equipe Técnica em sobre aviso	Custo total mensal por Equipe Técnica
OPERAÇÃO DE DATACENTER	09:00 às 18:00 horas X 5 dias	522	4	R\$ 55.327,54

INFRAESTRUTURA DE REDES E CONECTIVIDADE	09:00 às 18:00 horas X 5 dias	522	2	R\$ 37.625,63
TOTAL		522	2	R\$ 92.953,17

11.3.2.1.3. Em seguida, foi necessário calcular o custo médio da hora de serviço das equipes que possuem sobreaviso (D), dividindo o custo total mensal das equipes técnicas (A) pela multiplicação da quantidade total de perfis por categoria (B) pelo total de horas mensais por perfil, considerando 22 dias úteis (C), conforme a Tabela 11.06 a seguir.

Tabela 11.06. Custo médio da hora de serviço das categorias de serviços que possuem sobreaviso

Equipe Técnica	Custo total mensal das EQUIPE TÉCNICA (A)	Quantidade total de perfis por EQUIPE TÉCNICA (B)	Total de horas mensais por perfil considerando 22 dias úteis (C)	Custo médio da hora de serviço (D = A / (B x C)
OPERAÇÃO DE DATACENTER	R\$ 55.327,54	4	176	R\$ 78,59
INFRAESTRUTURA DE REDES E CONECTIVIDADE	R\$ 37.625,63	2	176	R\$ 106,89

11.3.2.1.4. Dessa forma, com o custo médio da hora de serviço calculado, foi possível estimar o custo total mensal para horas de sobreaviso (H), obtido pela multiplicação do custo médio da hora de serviço (D) pelo total de horas de sobreaviso mensais (F) e pelo fator de sobreaviso, equivalente a 1/3 da hora normal (G), conforme a Tabela 11.07.

Tabela 11.07. Custo total mensal das Horas de Sobreaviso

Equipe Técnica	Custo médio da hora de serviço (D)	Total de horas de sobreaviso mensais (F)	Fator de sobreaviso - 1/3 de hora (G)	Custo total mensal das horas de sobreaviso (H = D x F x G)
OPERAÇÃO DE DATACENTER	R\$ 78,59	522	0,33333333	R\$ 13.674,70
INFRAESTRUTURA DE REDES E CONECTIVIDADE	R\$ 106,89	522	0,33333333	R\$ 18.599,03
			TOTAL	R\$ 32.273,74

11.3.2.1.5. Portanto, o custo total mensal estimado para horas de sobreaviso das Equipe Técnicas que possuem cobertura de **sobreaviso** é de R\$ 32.273,74.

11.3.2.2. Custo total mensal estimado de horas extras de atividades realizadas fora da janela padrão

11.3.2.2.1. O cálculo do custo total mensal estimado para as horas extras de atividades realizadas fora da janela padrão (L) foi baseado na média das horas de atividades realizadas fora dessa janela no contrato atual, considerando os anos de 2024 e 2025, conforme detalhado na Tabela 11.08.

Tabela 11.08. Média de horas - atendimentos fora da janela padrão

	Requisição		Incidente		Mudança		
Mês/Ano	2024	2025	2024	2025	2024	2025	Total Geral Mês
Janeiro	0,00	5,60	0,00	0,00	0,00	0,00	5,60
Fevereiro	2,90	0,00	0,00	0,00	0,00	0,00	2,90
Março	0,00	0,00	3,50	0,00	10,00	0,00	13,50
Abril	2,80	4,10	0,00	0,00	8,00	0,00	14,90
Maiο	0,00	0,00	15,60	0,00	6,40	0,00	22,00
Junho	0,00	16,70	0,00	1,30	0,00	0,00	18,00
Julho	0,00	14,00	0,00	0,00	23,00	4,00	41,00
Agosto	0,00	13,20	18,90	0,00	14,90	10,70	57,70
Setembro	0,00	0,00	4,10	0,00	2,80	0,00	6,90
Outubro	8,10	7,50	0,00	4,50	0,00	1,60	21,70
Novembro	0,00	11,50	0,00	3,60	0,00	5,80	20,90
Dezembro	0,00	0,00	21,10	0,00	0,00	0,00	21,10
Média							20,52

11.3.2.2.2. Em seguida, para obter o custo total mensal estimado das horas extras de atividades realizadas fora da janela padrão (L), foi realizada a multiplicação do custo médio da hora de serviço (D) pela média de horas extras no período de jan-dez/2024 (I), e pelo fator de hora extra, equivalente a 1,5 (J), conforme a Tabela 11.09.

Tabela 11.09. Custo total mensal das Horas Extras – Dias da Semana

Equipe Técnica	Custo médio da hora de serviço (D)	Média de horas extras no período de 2024/2025 (I),	Fator de hora extra- 1,5 hora (J)	Custo total mensal das horas extras (L = D x I x J)
OPERAÇÃO DE DATACENTER	R\$ 78,59	20,5	1,5	R\$ 2.416,65
INFRAESTRUTURA DE REDES E CONECTIVIDADE	R\$ 106,89	20,5	1,5	R\$ 3.286,90
			TOTAL	R\$ 5.703,55

11.3.2.2.3. Portanto, o custo total mensal estimado para horas extras de atividades realizadas fora da janela padrão é de **R\$ R\$ 5.703,55**.

11.3.2.3. Assim, o custo da contratação após a adição dos outros itens de custo é apresentado na Tabela a seguir.

Custo total mensal estimado para o ITEM 01 quando inserido os valores estimados de custo com horas de sobreaviso e horas extras das Equipes Técnicas de "Operação de DataCenter" e “Infraestrutura de Redes e Conectividades”

11.3.2.3.1. A seguir, na Tabela 11.10, são apresentados os valores que compõem a estimativa de custo mensal após a inserção dos custos referentes à estimativa de horas de sobreaviso e horas extras das equipe técnicas.

Tabela 11.10. Valor mensal do ITEM 01 com horas de Sobreaviso e extras

Elementos de Custo Valores	Referência	Valor (R\$)
Estimativa de Custo Total Estimado da Equipe para o ITEM 01	Tabela 11.04	R\$ 610.311,81
Custo total mensal das Horas de Sobreaviso (ITEM 01)	Tabela 11.07	R\$ 32.273,74
Custo total mensal das Horas de Horas Extra - Dias da Semana (ITEM 01)	Tabela 11.09	R\$ 5.703,55
Valor mensal do ITEM 01 com horas de Sobreaviso e extras		R\$ 648.289,09

11.3.2.3.2. Portanto, o custo total mensal estimado para o ITEM 01 após as projeções de custo com horas de sobreaviso e horas extras para o ITEM 01 é de **R\$ R\$ 648.289,09**.

12. Descrição da solução de TIC a ser contratada

12.1. Cenário escolhido: Cenário 2 - Contratação por valor fixo mensal.

12.1.1. A solução de TIC consiste na prestação de serviços técnicos continuados especializados de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, presencial e remoto, mediante pagamento por valor fixo mensal, vinculado ao atendimento dos Indicadores de Níveis de Serviços e seus respectivos Níveis Mínimos de Serviço (NMS) estabelecidos no "Apêndice V - Indicadores de Níveis de Serviços" (SEI/ITI nº 0811192), conforme quantidades e perfis profissionais mínimos previstos em ordens de serviços, em conformidade com o modelo da Portaria nº SGD /MGI nº 1.070, de 1º de junho de 2023, compreendendo a disponibilização de:

12.1.1.1. Serviços continuados de atendimento, sustentação e suporte de TIC de nível 3 do modelo ITIL, considerando o monitoramento dos ativos e serviços críticos de TIC do ambiente computacional em regime 24x7x365;

12.1.1.2. Central de Serviços de TIC aderente ao modelo ITIL, compreendendo a configuração e a devida customização do sistema de controle de chamados ITSM (Sistema de Gerenciamento de Serviços de TI) já utilizados pelo ITI, considerando as ações de evolução contínua e os requisitos e especificações definidos;

12.1.2.3. Todos os elementos de software e hardware necessários ao bom desempenho dos serviços por parte dos profissionais alocados no que tange aos controles e rotinas internas da empresa e demais custos agregados, ressaltados os ativos disponibilizados pelo CONTRATANTE para operação, monitoramento e controle por parte das equipes;

12.1.2.4. Quantitativo e qualificação de profissionais compatível com a demanda, em conformidade com os itens abaixo, principalmente relacionadas à qualificação técnica comprovada por certificação e experiência profissional, bem como pela análise do Apêndices de I a VI, e mecanismos definidos para correta prestação dos serviços.

12.2. Serviços que compõem a Solução Escolhida

12.2.1 O certame será realizado em grupo e item único que contempla toda a prestação de serviço, uma vez que a Equipe de Planejamento da Contratação não identificou benefícios no parcelamento da solução, conforme detalhado nos itens 14 e 15 deste Estudo. Assim, a solução é composta pelos seguintes itens em grupo único:

Tabela 12.01. Itens para contratação

ITEM	DESCRIÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE (meses)
1	Serviços técnicos especializados de sustentação de infraestrutura crítica de TI	27014	Mês	24

12.3. Estrutura e Organização dos Serviços

12.3.1. Por se tratar de serviços com atividades especializadas, que necessitam de conhecimento específico da infraestrutura de TIC, o Órgão adotará o modelo estruturado em Equipes Técnicas (Squads), dessa forma, os perfis profissionais dimensionados para o atendimento da demanda, foram divididos em dez (10) Equipes Técnicas distintas, de modo a permitir o agrupamento de atividades com características e perfis profissionais similares. São elas:

- I. Governança de Serviços de TIC
- II. Operação de datacenter
- III. Sustentação de aplicações e banco de dados
- IV. Infraestrutura de redes e conectividade
- V. Cibersegurança
- VI. Gerenciamento e execução de serviços negociais DITEC
- VII. Gerenciamento e execução de serviços negociais DAFN

12.3.2. As definições e demais informações acerca destas Equipe Técnicas são apresentadas no "Apêndice III - Equipes Técnicas", deste estudo.

12.4. Modelo de Prestação dos Serviços

12.4.1. O modelo de Prestação dos serviços a serem executados pela CONTRATADA, a modalidade de remuneração, a disciplina do recebimento do objeto, os Níveis Mínimos de Serviços estabelecidos no "Apêndice V - Indicadores de Níveis de Serviços" (SEI/ITI nº 0811192) e "Apêndice VI - Especificações - Solução de Gerenciamento - ITSM" (SEI/ITI nº 0811325), e outros procedimentos previstos no Termo de Referência desta contratação.

12.5. Locais e Endereços da Execução dos Serviços

12.5.1. Os serviços serão prestados nas dependências do Instituto Nacional de Tecnologia da Informação, nos endereços apresentados na Tabela 12.06.

Tabela 12.02. Ambientes Tecnológicos do ITI

Referência	Descrição	Endereço	Tipo de Atendimento
CCD	Centro de Certificação Digital (CCD) do Instituto Nacional de Tecnologia da Informação (ITI)	Brasília / DF	Presencial e Remoto
Sede	Instituto Nacional de Tecnologia da Informação (ITI)	SAUS Quadra 06. Complexo-sede da Anatel, Bloco E, 8º Andar. Brasília - DF. CEP: 70070-940.	Presencial e Remoto
Contingência	Instituto Nacional de Tecnologia da Informação (ITI)	Rio de Janeiro - RJ.	Remoto

12.5.2. Os endereços constantes na Tabela 12.02, correspondem os possíveis locais de lotação dos profissionais alocados na prestação do serviço, podendo as atividades de escopo deste serviço serem desempenhadas para suporte remoto a quaisquer das localidades em que o ITI possua instalações de TIC.

12.5.3. A prestação do serviço deverá ser realizada conforme o regime estabelecido para cada perfil profissional dentro de sua respectiva Equipe Técnica conforme "Apêndice III - Equipes Técnicas".

12.5.4. Todos os custos inerentes aos deslocamentos necessários para o atendimento nas dependências e respectivas localidades, relacionadas na Tabela 12.02, serão de exclusiva responsabilidade da contratada.

12.6. Infraestrutura para Execução dos Serviços

12.6.1. Para os serviços executados nas dependências do Órgão, fica a cargo deste providenciar os recursos necessários ao bom desempenho deles, tais como: local de trabalho, móveis, ramais telefônicos e recursos computacionais (estações de trabalho, conexão à rede local e licenças de softwares).

12.6.2. Para os serviços executados fora das dependências do Órgão, os recursos de hardware e software, assim como quaisquer outros necessários, são de responsabilidade da CONTRATADA, incluindo telefones celulares para atendimento de acionamentos e a interconexão com a rede de dados da DITEC/ITI, assim como demais custos associados.

12.6.3. Caberá ao ITI apenas o fornecimento de software específico de acesso remoto seguro (Ex. VPN, ZTNA, etc) e de token para acesso remoto seguro ao seu ambiente.

12.6.4. O ITI poderá ainda, a seu exclusivo critério, ceder equipamentos com padrões específicos de segurança para uso pela CONTRATADA conforme a necessidade do serviço.

13. Estimativa de custo total da contratação

Valor (R\$): 15.558.938,16

13.1. A presente contratação tem custo estimado de **R\$ 15.558.938,16** (quinze milhões e quinhentos e cinquenta e oito mil e novecentos e trinta e oito reais e dezesseis centavos) **para período de execução contratual de vinte e quatro (24) meses, em conformidade com o disposto nesta seção.**

13.2. De forma que a Estimativa do Valor Mensal da Contratação, do Anexo I da Portaria SGD/MGI nº 1.070/2023, é apresentada na Tabela 13.01 a seguir.

Tabela 13.01. Estimativa do Valor Mensal da Contratação com projeções para 12 e 24 meses

ITEM	DESCRIÇÃO	CATSER	UNIDADE DE MEDIDA	Qtde.	Valor Estimado Mensal	Valor Estimado Total para 12 meses	Valor Estimado Total para 24 meses
1	Serviços técnicos especializados de sustentação de infraestrutura crítica de TI	27014	Unidade Mensal	24	R\$ 648.289,09	R\$ 7.779.469,08	R\$ 15.558.938,16

- 13.3. A estimativa de preços consta detalhada no "Apêndice VII - Planilha Simplificada para Estimativa do Valor", deste ETP.
- 13.3.1. A Planilha Simplificada para Estimativa do Valor Mensal do Serviço, apresenta os custos para a equipe estimada para esta contratação conforme valores publicados utilizando-se do fator K indicado no Anexo II da Portaria SGD/ME nº 1.070, de 1º de junho de 2023, e suas atualiza.
- 13.4. O serviço especificado prevê o atendimento em regime 24x7 a demandas urgentes em algumas categorias de serviço com Níveis Mínimos de Serviço (NMS) diferenciados, bem como a realização de atividades programadas fora da janela usual de serviço.
- 13.5. A ampliação do prazo de atendimento fora da janela de atendimento padrão da prestação do serviço tem como objetivo permitir o atendimento a demandas em regime de sobreaviso, sem a necessidade de alocação por parte da CONTRATADA de profissionais atuando de forma online ou presencial em regime 24x7, flexibilizando assim o modelo de prestação do serviço e trazendo economia para a administração pública. O acionamento desses profissionais ficará sob responsabilidade da ITI, que possui equipe específica para esta finalidade.
- 13.6. Especificamente para a Equipe Técnica de Cibersegurança, está prevista a alocação de profissionais por turno em escala 24x7x365, devido à necessidade de monitoramento contínuo do ambiente e dos serviços de tecnologia da informação do Órgão. Assim, foi considerado o custo do adicional noturno.
- 13.7. Dessa forma, além dos custos dos perfis profissionais previstos, a estimativa inclui:
- 13.7.1. Custo total mensal estimado para horas de sobreaviso das Equipes que possuem cobertura de sobreaviso;
- 13.7.2. Custo total mensal estimado de horas extras de atividades realizadas fora da janela padrão.

14. Justificativa técnica da escolha da solução

- 14.1. Para a contratação dos Serviços Técnicos Especializados de Operação de Infraestrutura de Tecnologia da Informação e Comunicação - TIC, a análise das soluções foi realizada e modelada pela Secretaria de Governo Digital do Ministério da Gestão e Inovação, nos termos da Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, atendendo as determinações do Tribunal de Contas da União, assim a presente contratação é modelada conforme referido normativo, por não se verificar situação de excepcionalidade na aplicação do modelo.
- 14.2. Da análise já apresentada, na qual as alternativas eram os Cenários 1 - Força de Trabalho Própria do Órgão e 3 - Contratação Direta das Empresas Públicas de TIC, optou-se, conforme já apontado, pelo Cenário 2 - Contratação por valor fixo mensal. O Cenário 2 está de tal forma consolidado no mercado nacional de serviços de tecnologia da informação na Administração Pública Federal, assim como atende ao modelo estabelecido na Portaria SGD/MGI nº 1.070, de 1º de junho de 2023.
- 14.3. Quanto ao Cenário 1, Força de Trabalho Própria do Órgão, conforme já indicado nos itens 9 e 10 deste Estudo, se observa como maior desvantagem, a redução da capacidade de gestão, além de adição de morosidade excessiva ao processo devido às necessidades de seleção e especialização de pessoal.
- 14.4. Já quanto ao Cenário 3, Contratação Direta das Empresas Públicas de TIC, não se vislumbrou vantagem que justificasse a restrição da competitividade caracterizada na alternativa escolhida.
- 14.5. A partir das propostas apresentadas, o Cenário 2, Contratação por valor fixo mensal, é a única capaz de incentivar a empresa contratada a otimizar os seus fluxos e procedimentos de resolução de requisições e incidentes para minimizar os problemas e seus impactos.
- 14.6. A mensuração do serviço com foco em indicadores de qualidade obtidos a partir do serviço prestado e da disponibilidade do ambiente de TI, provoca a empresa contratada a otimizar o ambiente de trabalho. O pagamento fixo mensal, obriga a empresa contratada a buscar uma maior automação do ambiente com o estabelecimento de procedimentos operacionais padrões e a devida documentação, dada a natureza da contratação baseada em punição à prestadora caso não sejam respeitados os indicadores de qualidade pré-estabelecidos. Em razão disso, o plano estratégico passa a ser a diminuição do esforço operacional com reflexos diretos em redução de custo e em um ambiente de TI mais estável, sendo possível mantê-lo com o

menor esforço possível. Diferentemente dos modelos que utilizam remuneração por unidades de serviços ou por chamados atendidos, o risco de haver necessidade de negociação de otimização de atividades rotineiras é reduzido, isso se deve ao fato de que a própria CONTRATADA terá interesse na melhoria dos processos.

14.7. Desta forma, conclui-se que há de se esperar melhores resultados quanto aos benefícios da contratação pelo modelo de valor fixo mensal vinculado a execução dos serviços a critérios objetivos de qualidade e resultados, frente aos possíveis riscos e respectivos efeitos negativos a que estão sujeitas as demais alternativas avaliadas.

14.8. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

14.8.1. A licitação será realizada em grupo e item único, não sendo possível o parcelamento. Isso se justifica pelo fato de que os Serviços Técnicos Especializados de Operação de Infraestrutura e Atendimento a Usuários de Tecnologia da Informação e Comunicação (TIC) constituem um conjunto indissociável, formado pela integração de serviços, sistemas, subsistemas e soluções tecnológicas que operam de maneira interdependente. Qualquer descontinuidade ou falha em um dos componentes pode comprometer a operacionalidade, a segurança e a disponibilidade do ambiente computacional como um todo, razão pela qual se exige a contratação em grupo único.

14.8.2. Em função de constituir solução de Tecnologia da Informação com alto grau de interação entre os serviços de sustentação à infraestrutura e suporte técnico, contendo características de especificidade, natureza contínua, complexidade e criticidade do ambiente e elevada exigência de níveis de qualidade requerida pelo negócio, entende-se que o parcelamento da contratação em grupos pode comprometer a sua satisfatória execução.

14.8.3. A opção pelo agrupamento dos itens está condizente, ainda, com a exceção disposta § 3º do art. 40 da Lei 14.133/2021:

"§ 3º O parcelamento não será adotado quando:

I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;

III - o processo de padronização ou de escolha de marca levar a fornecedor exclusivo."

14.8.4. Nesse sentido, o grupo único é mais satisfatório do ponto de vista da eficiência técnica, por manter a qualidade da Solução de TI, haja vista que o gerenciamento permanece todo o tempo a cargo de um mesmo administrador. Nesse ponto, as vantagens seriam o maior nível de controle pela Administração na execução dos serviços, a maior interação entre as diferentes fases da implantação/implementação, a maior facilidade no cumprimento do cronograma preestabelecido e na observância dos prazos, concentração da responsabilidade pela execução em uma só pessoa e concentração da garantia dos resultados.

14.8.5. A divisão do objeto em dois ou mais contratos especializados em Serviços Técnicos Especializados de Operação de Infraestrutura e Atendimento a Usuários de Tecnologia da Informação e Comunicação - TIC dificultaria a fiscalização e a responsabilização das empresas contratadas em casos de descumprimento dos acordos de nível de serviço (ANS), tendo em vista que as fronteiras entre as categorias de serviços e as respectivas atividades a serem executadas nem sempre são claramente definidas. Essa fragmentação acarretaria um aumento significativo na complexidade das atividades de fiscalização e na análise das justificativas apresentadas pelas contratadas, contrariando, assim, o princípio da eficiência que rege a Administração Pública.

14.8.6. Dessa forma, a adoção de um Lote Único visa assegurar maior controle sobre a execução do objeto contratual, promovendo melhor integração entre as diferentes fases da prestação dos serviços, redução da quantidade de servidores públicos necessários para as atividades de gestão e fiscalização contratual, e maior facilidade para o cumprimento das obrigações por parte da contratada.

14.8.7. O não parcelamento do objeto não restringe a competitividade do certame e nem traz prejuízo ao erário, visto que os itens que compõem o objeto são de mesma natureza e guardam relação entre si.

14.8.8. Nesse sentido, o ITI, em respeito à legislação vigente e na busca pela economicidade e na melhor forma de prestar os serviços, inclusive no que tange à garantia da padronização dos serviços, opta por contratar a solução por meio de um único prestador dos serviços.

15. Justificativa econômica da escolha da solução

15.1. Os critérios técnicos empregados para escolha da solução resultaram na seleção do cenário recomendado pela Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, cujo modelo de execução - obrigatório para os órgãos do SISP, nos termos do item 1.3 de seu Anexo I, valor fixo mensal vinculado a execução dos serviços a critérios objetivos de qualidade e resultados, já é o utilizado atualmente no contrato em execução em termos gerais que viabilizam o atendimento das necessidades atuais e agora, por meio da nova contratação, estarão adequados à Portaria vigente.

15.2. A presente contratação visa aprimorar a gestão, conformidade e maturidade do modelo de atendimento e de prestação dos serviços, alinhando-o, portanto, às diretrizes atuais.

15.3. Pode-se afirmar também que, com a atualização dos valores do Mapa de Pesquisa Salarial que integra a referida portaria, bem como do fator K a ser utilizado nas respectivas estimativas, materializados, por sua vez, com a publicação da Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, o montante calculado no presente estudo está de acordo com os valores atuais praticados no mercado.

15.4. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

15.4.1. O objeto da pretendida contratação, que forma o conjunto de serviços a serem contratados, configura uma Única solução de Tecnologia da Informação.

15.4.2. O grupo abarcou todos os elementos necessários para prover um único Serviço Técnico Especializado de Operação de Infraestrutura e Atendimento a Usuários de Tecnologia da Informação e Comunicação - TIC. Os itens que compõem o grupo representam os elementos necessários que em conjunto formam uma Única solução.

15.4.3. Considerando a dependência entre os itens que compõem o objeto desta contratação, comprovou-se economicamente inviável seu parcelamento, visto que a divisão do objeto pode comprometer o cumprimento dos requisitos técnicos apresentados neste artefato.

15.4.4. A contratação por grupo poderia causar prejuízo para a economia de escala, e tornaria inviável e prejudicial o bom desempenho da contratação, por se tratar de serviços complementares e indissociáveis.

15.4.5. A viabilidade econômica significa que o parcelamento deve trazer benefícios para a Administração, proporcionando um aumento da competitividade e uma consequente diminuição dos custos para a execução do objeto. No entanto, para uma real noção da viabilidade econômica do parcelamento, é preciso ter em mente a redução de custos proporcionada pela economia de escala ao se contratar o serviço em único lote.

15.4.6. Nesse sentido, o ITI, em respeito à legislação vigente e na busca pela economicidade e na melhor forma de prestar os serviços, inclusive no que tange à garantia da padronização dos serviços, opta por contratar a solução por meio de um único prestador dos serviços.

16. Benefícios a serem alcançados com a contratação

16.1. A contratação da empresa para atender às demandas apresentadas trará inúmeros benefícios significativos para a organização. Esses benefícios podem ser categorizados da seguinte forma:

16.1.1. **Suprimento de Necessidades Críticas de Pessoal:** O ITI atualmente enfrenta desafios consideráveis em termos de recursos humanos, conforme identificado no Plano de Gestão de Pessoas do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). A contratação de uma empresa de TI permitirá suprir as necessidades de pessoal qualificado de maneira ágil e eficaz. Isso garantirá o acesso imediato a profissionais experientes em serviços, sistemas, infraestrutura, governança de TIC, segurança, pessoal e capacitação, alinhando-se assim com as metas e ações do PDTIC.

16.1.2. **Atendimento às Recomendações do CNJ:** A metodologia proposta pelo Conselho Nacional de Justiça (CNJ), conforme estabelecida na Resolução 90 de 29 de setembro de 2009, é utilizada como referência para dimensionar a força de trabalho mínima necessária na área de TIC. A contratação de uma empresa de TI permitirá que o ITI alcance o quantitativo recomendado de profissionais de TI de acordo com a metodologia do CNJ. Isso é fundamental para garantir o funcionamento eficiente dos serviços de tecnologia da informação e comunicação, atendendo às demandas internas e aos padrões estabelecidos.

16.1.3. **Foco nas Atividades Estratégicas:** A disponibilidade de profissionais de TI contratados por meio da empresa especializada permitirá que as diretorias envolvidas se concentrem nas atividades estratégicas e de gestão da área de TIC. Isso possibilitará o atendimento de forma mais eficiente às necessidades da organização, garantindo o alinhamento com as metas e ações do PDTIC. Além disso, as funções gerenciais e estratégicas da área de TIC poderão ser executadas por profissionais efetivos e qualificados, otimizando o desempenho institucional.

16.1.4. **Agilidade na Resposta às Demandas de TIC:** A contratação de uma empresa de TI proporcionará flexibilidade necessária para atender às demandas de TIC de forma ágil e responsiva. Isso é crucial em um ambiente em constante evolução, onde as necessidades de tecnologia podem surgir rapidamente. A empresa de TI poderá alocar recursos de acordo com demandas específicas, garantindo que os projetos sejam concluídos dentro dos prazos estabelecidos.

16.2. Em resumo, a contratação de uma empresa de TI apresenta benefícios substanciais, permitindo o atendimento eficiente das necessidades de pessoal, a conformidade com as diretrizes do ICP-Brasil, a concentração nas atividades estratégicas e a agilidade na resposta às demandas de TIC. Isso contribuirá significativamente para o alcance das metas e ações estabelecidas no PDTI e para a melhoria contínua dos serviços de tecnologia da informação e comunicação na organização.

16.3. Em síntese, o atendimento às necessidades de negócio e tecnológicas irão refletir a transição para um modelo integrado, inteligente e orientado a resultados. A contratação proposta consolidará uma nova arquitetura de serviços de TIC baseada em observabilidade, automação, segurança e governança, assegurando disponibilidade contínua, resiliência e alinhamento estratégico à missão institucional de promover a confiança digital no Brasil.

16.4. Essa nova arquitetura de serviços deverá proporcionar uma visão unificada e inteligente do ambiente tecnológico, reduzindo riscos, acelerando respostas e consolidando o ITI como referência em governança e excelência operacional no setor público digital.

16.5. Consolidando Expectativas de Valor e Resultados Institucionais

- Aumentar a disponibilidade e confiabilidade dos serviços digitais críticos, assegurando níveis de serviço compatíveis com as exigências da ICP-Brasil e da EAT;
- Promover automação, padronização e visibilidade operacional, reduzindo o tempo de resposta a incidentes e o custo de operação;

- Consolidar um modelo de operação tecnológica moderno e orientado a resultados, com métricas e SLAs claros, reduzindo riscos operacionais e fortalecendo a governança;
- Fortalecer a conformidade técnica e normativa, garantindo auditorias bem-sucedidas e aderência aos padrões nacionais e internacionais;
- Melhorar a capacidade institucional de planejamento e evolução tecnológica, em alinhamento com os objetivos estratégicos do Instituto e com a política de transformação digital do Governo Federal.

16.6. A pretensa contratação deverá entregar resultados concretos, mensuráveis e focados na melhoria da qualidade do serviço.

Tabela 16.01. Resultados Esperados

Objetivo de Negócio	Resultado Específico Esperado
Disponibilidade e Resiliência	Aumento na disponibilidade dos serviços e sistemas críticos, com pronto restabelecimento por meio de adequado gerenciamento de incidentes e problemas.
Qualidade e Eficiência	Cumprir os Níveis Mínimos de Serviços (NMS) estabelecidos e promover a racionalização de recursos e a melhoria contínua dos serviços.
Segurança e Privacidade	Assegurar o adequado tratamento de dados pessoais e informações classificadas (em conformidade com a LGPD), bem como aprimorar os mecanismos de segurança da informação.
Maturidade e Governança	Adoção de práticas de gestão e controle baseadas em ITIL v4, COBIT 2019 e ISO/IEC 20000-1, resultando na elevação da maturidade operacional e na transparência dos serviços (via dashboards e relatórios de NMS/KPIs).
Experiência do Usuário	Crescimento do grau de satisfação dos usuários de TI, com o aprimoramento da percepção de valor e a promoção da gestão da Experiência do Usuário.
Apoio Estratégico	Apoiar técnica e operacionalmente a elaboração de normas, procedimentos, projetos, contratações e a prospecção de novas tecnologias, potencializando a entrega de valor para o cidadão por meio da otimização da infraestrutura.

17. Providências a serem Adotadas

17.1. Para a presente contratação serão adotadas as seguintes providências:

- Levantamento de Requisitos: Identificação das necessidades e especificações técnicas.
- Elaboração do Termo de Referência: Documento que detalha os requisitos, escopo e condições da contratação.
- Elaboração de Mapa de Risco para o cenário escolhido neste estudo.
- Processo de Seleção: Publicação de edital e seleção da empresa fornecedora.
- Implementação e Gestão do Contrato: Acompanhamento da execução dos serviços e gestão do contrato conforme as cláusulas estabelecidas.

17.2. Assim, a Equipe de Planejamento da Contratação, com base no dimensionamento dos serviços e na complexidade do objeto a ser contratado, estima a necessidade de um quadro mínimo de quatro (04) servidores públicos para a gestão e fiscalização dos serviços a serem contratados.

Tabela 17.01. A distribuição dos servidores necessário a Gestão do Contrato

Unidade de Lotação	Quantidade de Servidores	Função Exercida
Coordenação-Geral de Infraestrutura e Segurança (CGISE / DITEC)	2	1 Gestor e 1 Fiscal Técnico
Coordenação de Licitações e Contratos (COLIC / DPOA)	1	Fiscal Administrativo
Diretoria de Auditoria, Fiscalização e Normatização (DAFN)	1	Fiscal Setorial

17.3. Esses servidores devem possuir conhecimentos especializados em suas áreas de atuação, além de experiência em fiscalização e gestão de contratos de TIC. Em adição, tem sido adicionado ao Plano de Desenvolvimento de Pessoas (PDP) da instituição a demanda por qualificação da equipe para atuar na gestão e fiscalização do contrato.

17.4. Considerando se tratar de serviço que já é prestado, não há providências a serem adotadas quanto a adequação do ambiente do órgão para viabilizar a execução contratual.

18. Contratações Correlatas/Interdependentes

18.1. Não existem contratações correlatas ou interdependentes em curso, porque essa contratação é autocontida não necessitando de outros itens para que se conclua a sua execução contratual.

18.2. Os itens listados foram elaborados levando em consideração todas as necessidades atuais do Órgão.

19. Declaração de Viabilidade

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

19.1. Justificativa da Viabilidade

19.1.1. O Estudo Técnico Preliminar desta contratação demonstra que a alternativa mais adequada para o atendimento da necessidade identificada, com mitigação de riscos e aderência aos princípios de economicidade, eficiência e efetividade, consiste na adoção do "Cenário 2 – Contratação por valor fixo mensal".

19.1.2. Tal abordagem mostrou-se a mais vantajosa dentre as alternativas avaliadas, desde que observadas as premissas, critérios e conclusões estabelecidos neste Estudo, em conformidade com a Instrução Normativa SGD nº 94, de 23 de dezembro de 2022.

19.2. Benefícios esperados da contratação

19.2.1. Continuidade e confiabilidade operacional: A contratação permitirá assegurar o funcionamento contínuo, seguro e eficiente dos sistemas e serviços de TIC essenciais à atividade institucional, garantindo elevados níveis de disponibilidade e acesso a suporte técnico especializado. Adicionalmente, possibilitará a atuação proativa na prevenção, detecção, resposta e mitigação de incidentes de segurança, reforçando os princípios de confidencialidade, integridade, disponibilidade e autenticidade da informação, fundamentais para a prestação de serviços públicos digitais.

19.2.2. Eficiência operacional e otimização de recursos: A adoção de serviços especializados contribuirá para a redução de retrabalho, indisponibilidades e intervenções corretivas emergenciais,

promovendo maior previsibilidade operacional. Ademais, permitirá a otimização do uso dos recursos humanos internos, com redirecionamento das equipes para atividades estratégicas e melhoria nos tempos de resposta a incidentes.

19.2.3. Aumento da maturidade em segurança da informação: A contratação proporcionará avanço estruturado e mensurável na maturidade da segurança da informação institucional, mediante a adoção de práticas e controles alinhados a referências reconhecidas internacionalmente, tais como ISO/IEC 27001, NIST e CIS. Adicionalmente, a inclusão de ações de capacitação e transferência de conhecimento contribuirá para a sustentabilidade das melhorias implementadas e para o fortalecimento contínuo da governança de segurança da informação.

19.2.4. Economicidade e racionalização do gasto público: O cenário proposto apresenta maior vantagem sob o ponto de vista econômico, considerando o custo total de propriedade (TCO) da solução, baseado em modelo de contratação com pagamento mensal fixo vinculado a Indicadores de Níveis de Serviço (INS). A abordagem baseada em serviços gerenciados permite:

- redução de custos com aquisições isoladas de tecnologia (CAPEX);
- previsibilidade orçamentária;
- diminuição de gastos com manutenções corretivas e emergenciais;
- mitigação de impactos operacionais e reputacionais decorrentes de incidentes de segurança;
- contribui para a conformidade com a LGPD e demais normativos da Administração Pública Federal, reduzindo potenciais passivos jurídicos e fortalecendo a estabilidade institucional.

19.3. Conclusão de viabilidade

19.3.1. Diante do exposto, conclui-se que a contratação de serviços gerenciados de segurança da informação:

- é tecnicamente viável;
- está estrategicamente alinhada às diretrizes institucionais e normativas;
- apresenta-se economicamente vantajosa;
- e atende aos requisitos estabelecidos na IN SGD nº 94/2022.

19.3.2. A solução proposta contribui diretamente para o fortalecimento da governança de TIC, da resiliência cibernética e da continuidade dos serviços públicos digitais sob responsabilidade do órgão.

19.4. Declaração da equipe de planejamento

19.4.1. Dessa forma, a equipe de planejamento manifesta-se favorável à contratação do cenário proposto, por entendê-lo como o mais adequado para o atendimento da necessidade institucional, observados os requisitos técnicos, operacionais e normativos pertinentes.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

Despacho: Portaria 48/2026 - EPC (0798941)

ALYSSON MARQUES

Integrante Requisitante



Assinou eletronicamente em 01/09/2026 às 18:25:47.

Despacho: Portaria 48/2026 - EPC (0798941)

RAFAEL DE LIMA RAMOS

Integrante Técnico



Assinou eletronicamente em 03/09/2026 às 14:46:30.

Despacho: Diretor de Infraestrutura Tecnológica - DITEC Portaria SRI/Casa Civil/PR Nº 270, de 10 de MARÇO de 2025

JOSE RODRIGUES GONCALVES JUNIOR

Autoridade Máxima de TIC



Assinou eletronicamente em 01/09/2026 às 14:58:09.

Despacho: Portaria 48/2026 - EPC (0798941)

MATHEUS MARQUES DA SILVA

Integrante Administrativo



Assinou eletronicamente em 03/09/2026 às 14:23:38.

LICITAÇÃO: ANEXO Nº ETP 6/2026 - APÊNDICE I -/2026/ASSESSOR-DITEC/DITEC

Processo nº 00100.002198/2025-02

Interessado: CGISE

APÊNDICE I - INFRAESTRUTURA DE TIC

1. AMBIENTES CIBERNÉTICOS

Referência	Descrição	Endereço
Sede	Instituto Nacional de Tecnologia da Informação (ITI)	SAUS Quadra 06. Complexo-sede da Anatel, Bloco E, 10º Andar. Brasília - DF. CEP: 70070-940.
CCD	Centro de Certificação Digital (CCD)	Endereço a ser informado no ato da contratação. Brasília - DF
Contingência	Site Contingência	Endereço a ser informado no ato da contratação. Rio de Janeiro - RJ

1.1. SEDE

- I - Atividades desempenhadas: Atividades Administrativas e Técnicas (Regime Remoto e Presencial)
- II - Equipe Presencial: Sim
- III - Dispositivos e Equipamentos:
 - a) Estações de trabalho
 - b) Servidores
 - c) Switchs
 - d) HSM
 - e) Storage

1.2. CCD

- I - Atividades desempenhadas: Atividades Administrativas e Técnicas (Regime Remoto e Presencial)
- II - Equipe Presencial: Sim
- III - Dispositivos e Equipamentos:

- a) Estações de trabalho
- b) Servidores
- c) Switches
- d) Roteadores para acesso a rede Internet e Intranet a partir da rede mundial de computadores
- e) HSM (Módulo de Segurança de Hardware) - Equipamentos criptográficos para armazenamento de chaves
- f) Storages e equipamento de armazenamento de dados através da rede SAN e/ou LAN
- g) Controle de acesso biométrico, câmeras, fechaduras, sensores e leitores.
- h) Firewalls de borda e intranet

1.3. Contingência

- I - Atividades desempenhadas: Atividades Técnicas (Regime Remoto)
- II - Equipe Presencial: Não
- III - Dispositivos e Equipamentos:
 - a) Estações de trabalho
 - b) Servidores
 - c) Switches
 - d) Roteadores para acesso a rede Internet e Intranet a partir da rede mundial de computadores
 - e) HSM (Módulo de Segurança de Hardware) - Equipamentos criptográficos para armazenamento de chaves
 - f) Storages e equipamento de armazenamento de dados através da rede SAN e/ou LAN
 - g) Controle de acesso biométrico, câmeras, fechaduras, sensores e leitores.
 - h) Firewalls de borda e intranet

2. DESCRIÇÃO DO AMBIENTE TECNOLÓGICO - DITEC

2.1. HARDWARE

- 2.1.1. Estações de Trabalho (Workstations, Desktops e Notebooks): Mais de 35 estações de trabalho entre workstations, notebooks e desktops físicos e virtuais.
- 2.1.2. Servidores: Aproximadamente 374 servidores virtualizados. Entre 54 ou mais servidores físicos distribuídos em quatro sites, sendo três em Brasília e um no Rio de Janeiro
- 2.1.3. Hardwares Criptográficos: Mais de 20 HSMs
- 2.1.4. Equipamentos de Rede: Entre 17 ou mais switches do tipo SAN e LAN. No mínimo 4 firewalls de borda e outros internos para segregação da LAN.
- 2.1.5. Redes de Computadores e Conectividade
 - I - Arquitetura - Rede de dados LAN, MAN e WAN, com uso de acesso a sites remotos na mesma cidade, bem como em cidades geograficamente distintas.

II - Protocolos, Ethernet, TCP/IP, PPP/PPTP, MPLS, SDWAN, e similares

III - Link(s): 3 a 4 links de Internet (Sites Brasília e site Rio de Janeiro). 4 a 8 firewalls (Borda e Intranet para Sites Brasília e site Rio de Janeiro)

2.1.6. Redes de Dados (SAN) / Arquitetura: 4 Storages de armazenamento de dados do tipo bloco e objeto. 7 Switches SAN para comunicação de bloco de dados sobre fibra ótica (FC).

2.2. **VIRTUALIZAÇÃO E CONTÊINERES**

2.2.1. Tecnologia

I - Virtualização atual baseada em Vmware e ProxMox, KVM, Virtualbox, e demais tecnologias similares de virtualização bare-metal, hospedados ou de para virtualização, bem como de camada de tradução similares ao Wine ou de emulação.

II - Containerização com utilização de tecnologias de acesso privilegiado e segregação de contextos no núcleo do sistema operacional, para execução de containeres, similares ao Containerd, CRI-O, Podman e demais compatíveis às tecnologias adotadas pelo Kubernetes, Rancher, OpenShift.

III - Armazenamento de dados distribuídos em formato de bloco, objeto ou arquivo do tipo Ceph, Longhorn, ZFS, Rook, MinIO, S3 e demais tecnologias similares.

2.2.2. Quantitativos

I - Aproximadamente 24 servidores físicos

II - Aproximadamente 374 servidores virtuais.

III - Aproximadamente 5 ambientes de containerização.

2.3. **DOCUMENTAÇÃO, GESTÃO DE PROCESSOS E CONHECIMENTO**

2.3.1. Gestão de Documentação Técnica

I - Elaborar e manter repositórios organizados com registros técnicos, arquiteturas de sistemas, especificações, manuais e artefatos de projeto.

II - Disponibilizar e versionar documentos oficiais em plataformas internas de armazenamento institucional.

2.3.2. Gestão de Processos de TIC

I - Mapear, formalizar e manter atualizados os fluxos operacionais e administrativos relacionados às atividades de TIC.

II - Apoiar na elaboração de documentos que definam etapas, responsáveis, prazos e indicadores de desempenho dos processos de TI.

2.3.3. Gestão de Conhecimento Institucional

I - Registrar e manter atualizadas as lições aprendidas, resoluções de incidentes, boas práticas e instruções operacionais recorrentes.

II - Promover e manter iniciativas de disseminação do conhecimento técnico entre os integrantes da equipe, com foco em padronização e capacitação.

2.3.4. Controle de Manuais e Procedimentos

- I - Elaborar, revisar e manter atualizados manuais operacionais, guias de usuário, instruções de trabalho e procedimentos técnicos.
- II - Disponibilizar os documentos controlados em repositório institucional com controle de versão, revisões aprovadas e acesso estruturado às equipes da DITEC.

2.4. **SISTEMAS E SOFTWARES**

2.4.1. Sistemas de Gestão de Banco de Dados (SGBD): Incluindo, mas não se limitando a PostgreSQL, MySQL/MariaDB, SQL Server, MongoDB.

2.4.2. Sistemas de Gestão de Infraestrutura: Incluindo, mas não se limitando a Zabbix, Grafana, Prometheus, ELK Stack.

2.4.3. Sistemas de Gestão de Mudança: Incluindo, mas não se limitando a GLPI, ServiceNow, Jira Service Management.

2.4.4. Sistemas de Controle de Versionamento: Incluindo, mas não se limitando a GitLab, GitHub, Bitbucket, SVN.

2.4.5. Sistemas de Monitoramento e Observabilidade: Incluindo, mas não se limitando a Grafana, Prometheus, Zabbix, Datadog, Elastic APM, Opensearch, Graylog.

2.4.6. Sistemas de Arquiteturas Distribuídos e Balanceamento de Carga: Incluindo, mas não se limitando a F5 BIG-IP, NGINX, HAProxy, Traefik, NGINX, MetalLB.

2.4.7. Softwares de Operação / Sistemas Operacionais: Incluindo, mas não se limitando a Linux (CentOS, RHEL, Ubuntu), Windows Server, BSD (OpenBSD, FreeBSD).

2.4.8. DevOps:

- I - Versionamento: Incluindo, mas não se limitando a GitLab, SVN;
- II - Orquestração de Contêineres: Incluindo, mas não se limitando a Rancher, Kubernetes, Docker, Podman, Tanzu OpenShift;
- III - Infraestrutura como Código (IaC): Incluindo, mas não se limitando a Ansible, Puppet, Terraform, Chef, Salt;
- IV - CI/CD: Incluindo, mas não se limitando a Jenkins, GitLab CI, ArgoCD, Tekton;
- V - Repositório de Imagens: Incluindo, mas não se limitando a Harbor, Nexus, Artifactory.

2.4.9. Segurança: Sistemas de gestão de incidentes e vulnerabilidades, incluindo, mas não se limitando a Greenbone, Graylog, MISP, Wazuh, Tenable, SolarWinds, Snort, Datadog.

2.4.10. Monitoramento: Incluindo, mas não se limitando a Zabbix, Prometheus, Opensearch, Grafana, Nagios, Qualys, Rapid7

2.4.11. Aplicações Corporativas

- I - Assinador (Assinaturas digitais do tipo Avançada e Qualificada)
- II - Validador (Verificador de assinaturas - Validar)
- III - LCR (Lista de Certificados Revogáveis)
- IV - Sistemas de gestão de identidades (Apareo CAS, Keycloak, e

outros) Login Universal – Gerenciamento de Identidades e Acessos

V - Banco de Dados Centralizado

VI - SAF - SISTEMA ANTI-FRAUDE

VII - SGC2 - SISTEMA GERENCIADOR DE CERTIFICADOS

VIII - Sistema Biometria (Base: AIRFLOW) - Plataforma de código aberto para criar, agendar e monitorar fluxos de trabalho (workflows) como Código.

IX - CAR - CADASTRO DE AGENTES DE REGISTRO

X - SISTEMA DE AUDITORIA - SISTEMA PARA CADASTRAMENTO DOS RELATÓRIOS DE AUDITORIA OPERACIONAL

XI - CASA - CADASTRO DE ENTIDADES DA ICP BRASIL

2.4.12. Sites, Portais e Painéis Web, incluindo, mas não se limitando:

I - <https://meucertificado.it.gov.br/>

II - <https://validar.it.gov.br/>

III - <https://validar.it.gov.br/>

IV - <https://assinador.it.gov.br/>

V - <https://numeros.it.gov.br/>

VI - <https://fila.it.gov.br/>

VII - <https://auditoria-externo.it.gov.br/>

VIII - <https://fiscalizacao.it.gov.br/>

IX - <https://listaars.it.gov.br/>

X - <https://estrutura.it.gov.br/>

2.5. **QUADROS RESUMO - ATIVOS DE TIC**

2.5.1. GERENCIAMENTO DE SERVIÇOS DE TIC

ID	NOME DO ATIVO	DESCRIÇÃO DO ATIVO	QUANTIDADE
1	OTRS	Open Source Ticket Request System	3

2.5.2. SUSTENTAÇÃO DE APLICAÇÕES

ID	NOME DO ATIVO	DESCRIÇÃO DO ATIVO	QUANTIDADE
1	Virtualização	Vmware	22
		ProxMox	2
2	Servidores	Físicos	54
		Virtuais	374
3	Sistema Operacional	Windows	11
		Linux	370
		BSD/Unix	25
		Apache	13
		Tomcat	6

4	Servidores Web		
		Nginx	9
		Node.js	2
		Haproxy	6
		Wildfly	6
5	Infraestrutura em Containers	Grafana, Graylog, Fluentd OpenSearch, EKS	5
		Gitlab, Github, Registries, Nexus	2
6	DevOps e DevSecOps	Rancher, Docker, Podman, Kubernetes	25
		Jenkins, Git, Bootstrap, VScode, PyCharm	3
		Trivy, Clair, Snyk, Grype, Wazuh, Suricata	20
7	Infraestrutura como Código (IaC)	Ansible, Gitlab, Salt, Vagrant	4
		Git-runner	40

2.5.3. ARMAZENAMENTO E BACKUP

ID	NOME DO ATIVO	DESCRIÇÃO DO ATIVO	QUANTIDADE
1	Backup	Veeam	2
		Bacula	3
2	Storage	Huawei	2
		Dell EMC	3

2.5.4. SUSTENTAÇÃO DE BANCO DE DADOS

ID	NOME DO ATIVO	DESCRIÇÃO DO ATIVO	QUANTIDADE
1	Sistema de Gerenciamento de Banco de Dados (SGBD)	SQL Server	2
		PostgreSQL	15
		MySQL/MariaDB	8

2.5.5. SEGURANÇA DE TIC

ID	NOME DO ATIVO	DESCRIÇÃO DO ATIVO	QUANTIDADE
1	Firewall	Fortinet	4
		PacketFilter (OpenBSD PF)	2
2	IDS/IPS	Wazuh	1
		Suricata	20
		Snort	4
3	Cofre de Senhas	Syspass	2
4	HSM	Módulo de Segurança de Hardware / Hardware Criptográfico	20

2.5.6. CONECTIVIDADE E COMUNICAÇÃO

ID	NOME DO ATIVO	DESCRIÇÃO DO ATIVO	QUANTIDADE
1	Domínio de autenticação	LDAP	4
2	DNS	DNS Interno	6
		DNS Externo	6
3	Redes	Switchs	17
		Vlans	13
		Link WAN	4
4	NTP	NTP Interno	2
		NTP Externo	3
5	Servidor de E-mail	Interno	2
		Externo	2

2.5.7. MONITORAMENTO DE SERVIÇOS DE TIC

ID	NOME DO ATIVO	DESCRIÇÃO DO ATIVO	QUANTIDADE
1	Grafana	Visualização gráfica	2
2	Zabbix	Monitoramento de Ativos	3
3	Nagios	Monitoramento de Ativos	2
4	Opensearch	Consulta e pesquisa de logs	2
5	Graylog	Consulta e pesquisa de logs	2
6	Metabase	Consulta de informações de BI	2

7	Prometheus	Métricas de sistemas	2

2.5.8. SUPORTE TÉCNICO DE MICROINFORMÁTICA

ID	NOME DO ATIVO	DESCRIÇÃO DO ATIVO	QUANTIDADE
1	Sistema Operacional	Windows	35
2	Estações de trabalho	Desktop	30
		Notebook	5



Documento assinado eletronicamente por **Rafael de Lima Ramos, Coordenador(a)**, em 01/09/2026, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Alysson Marques, Coordenador-Geral**, em 01/09/2026, às 11:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0810756** e o código CRC **3C7DD682**.

LICITAÇÃO: ANEXO Nº ETP 6/2026 - APÊNDICE II -/2026/ASSESSOR-DITEC/DITEC

Processo nº 00100.002198/2025-02

Interessado: CGISE

APÊNDICE II - CATÁLOGO DE SERVIÇOS

1. DISPOSIÇÕES GERAIS

A Diretoria de Infraestrutura Tecnológica (DITEC), como Unidade Organizacional do Instituto Nacional de Tecnologia da Informação (ITI) é responsável pela operacionalização da Autoridade Certificadora Raiz (AC Raiz) da ICP-Brasil e o provimento de Serviços Negociais/Finalísticos, a exemplo do serviço de Assinaturas Eletrônicas Avançadas.

É crucial que o Catálogo de Serviços descreva o que e como a organização atende as demandas dos usuários.

Diante da necessidade institucional, este catálogo apresenta, juntos, os Catálogos de Serviços elaborados. De forma que este foi dividido como:

Catálogo de Serviços Negociais: contém todos os serviços de TIC em operação e disponíveis para os clientes ou sendo preparados para serem entregues aos clientes; e

Catálogo de Serviços Técnicos: contém todas as requisições de serviço disponíveis para os clientes e usuários de serviços de TIC.

2. CATÁLOGO DE SERVIÇOS NEGOCIAIS

O Catálogo de Serviços da Diretoria de Infraestrutura Tecnológica (DITEC) deve listar os serviços centrados no negócio que entregam valor aos clientes internos e externos do Instituto Nacional de Tecnologia da Informação (ITI).

Este catálogo é estruturado com base nas melhores práticas internacionais, como a ABNT NBR ISO/IEC 20000-1:2020, e nas diretrizes federais para contratação de serviços de operação de infraestrutura e atendimento a usuários de TIC.

Quadro resumo de Serviços Negociais

ID	Nome do Serviço
S-01	Operação e Disponibilidade da AC Raiz da ICP-Brasil
S-02	Assinaturas Eletrônicas Avançadas

S-03	Validação de Conformidade Digital
S-04	Auditoria e Sincronização de Tempo
S-05	Gestão e Publicação da Lista de Confiança
S-06	Operação de Infraestrutura Tecnológica (Nível 3)
S-07	Serviços de Inteligência e Análise Preditiva em apoio as atividades de Auditoria e Fiscalização
S-08	Serviço de Sustentação dos sistemas de combate à fraude da ICP Brasil

Cada serviço apresenta uma matriz RACI que deve ser preenchida considerando “APÊNDICE A - LISTA DE PARTES INTERESSADAS E APROVADORES” deste documento:

- **R (Responsible) - Responsável (quem executa):** São as pessoas ou equipes que realizam o trabalho. Executam atividades, tarefas e entregas. Há pelo menos um “R”, mas pode haver vários.
 - Ex.: Equipes técnicas, as Áreas de Atuação (squads) que executam o serviço.
- **A (Accountable) - Aprovador / Responsável Final (quem responde pelo resultado):** É quem presta contas, tem autoridade e “assina embaixo”. Apenas uma pessoa ou unidade deve ter esse papel por serviço. Decide, aprova e valida a entrega final.
 - Ex.: Direção da DITEC, CGOPE, CGISE, e DAFN (quando regulatório).
- **C (Consulted) - Consultado (quem orienta, contribui, revisa):** Envolve especialistas, órgãos reguladores ou partes impactadas. Interação antes ou durante a execução. É sempre uma comunicação bidirecional.
 - Ex: Comitê Gestor da ICP-Brasil, Auditoria, Órgãos integrados, entidades da ICP-Brasil.
- **I (Informed) - Informado (quem deve ser comunicado):** Recebe avisos, relatórios e atualizações. Não participa da execução nem da decisão. Comunicação unidirecional.
 - Ex.: Usuários internos, clientes Gov.br, integradores via API e demais diretorias.

Sobre a Governança:

I - Responsáveis

- a) Responsável pelo Catálogo: DITEC
- b) Co-responsáveis: CGISE, CGOPE, DAFN
- c) Responsáveis pela aprovação: Direção da DITEC

II - Periodicidade

Revisão **semestral ou diante de** mudanças críticas

III - Fluxo de alteração

2.1.

S-01 - Operação da AC Raiz da ICP-Brasil

ID do Serviço	S-01
Nome do Serviço (Resultado Pretendido)	Operação da AC Raiz da ICP-Brasil
Descrição do Serviço e Alinhamento ao ITI	Operação da Autoridade Certificadora Raiz (AC Raiz) visa a garantia da operação ininterrupta (24x7x365) da infraestrutura de <i>hardware</i> e <i>software</i> que suporta as funções críticas da AC Raiz, incluindo a revogação de certificados e a geração/publicação da Lista de Certificados Revogados (LCR). A operação deve estar em Ambientes Seguros (Salas Cofre/CCD).
Base Normativa de Suporte e outras informações	Funções críticas da ICP-Brasil. Disponibilidade do serviço ≥ 99,99%. Conformidade com os requisitos de segurança física e lógica do DOC-ICP-01 e DOC-ICP-02. Além de outras Diretrizes do Comitê Gestor da ICP-Brasil.

Matriz RACI

Função RACI	Descrição
R - Responsible	Equipes Técnicas (<i>squads</i>): Governança de Serviços de TIC, Operação de Datacenter, Sustentação de aplicações e banco de dados, Infraestrutura de redes e conectividade, Cibersegurança, Gerenciamento e Execução de Serviços Negociais DITEC, Gerenciamento e Execução de Serviços Negociais DAFN. Gerencial: COICP; COTEC; COSEG
A - Accountable	CGOPE
C - Consulted	Comitê Gestor ICP-Brasil; Auditoria Interna; Entidades ICP-Brasil
I - Informed	Usuários internos; Ecossistema ICP-Brasil; Demais Diretorias do ITI

2.2.

S-02 - Serviço de Assinaturas Eletrônicas Avançadas

ID do Serviço	S-02
Nome do Serviço (Resultado Pretendido)	Serviço de Assinaturas Eletrônicas Avançadas

Descrição do Serviço e Alinhamento ao ITI	Provimento das Assinaturas Eletrônicas Avançadas do Gov.br e gestão dos acessos por API, incluindo manutenção de chaves em ambiente seguro. Operação contínua da infraestrutura tecnológica (<i>hardware, software, storages, redes</i>), inclui a Manutenção das Chaves em Ambiente Seguro (Salas Cofre).
Base Normativa de Suporte e outras informações	Normas do Gov.br; Diretrizes da ICP-Brasil; Regras de operação da AC Raiz. Sustentação dos serviços essenciais. Tempo Máximo de Indisponibilidade (MTBF) do serviço de Assinatura Avançada. Execução das rotinas de replicação de dados entre sítios de redundância

Matriz RACI

Função RACI	Descrição
R - Responsible	Equipes técnicas (Squads): Governança de Serviços de TIC, Operação de Datacenter, Sustentação de aplicações e banco de dados, Infraestrutura de redes e conectividade, Cibersegurança, Gerenciamento e Execução de Serviços Negociais DITEC. Gerencial: COSES; COTEC; COSEG
A - Accountable	COSES
C - Consulted	SGD/MGI; Órgãos integrados
I - Informed	Usuários externos Gov.br; Integradores API

2.3.

S-03 - Serviço de Validação de Conformidade Digital

ID do Serviço	S-03
Nome do Serviço (Resultado Pretendido)	Serviço de Validação de Conformidade Digital
Descrição do Serviço e Alinhamento ao ITI	Validação e verificação de conformidade de assinaturas digitais ICP-Brasil conforme DOC-ICP-15, incluindo serviços via API. Manutenção da infraestrutura para os serviços e desenvolvimento de projetos de validação de assinaturas eletrônicas.
Base Normativa de Suporte e outras informações	DOC-ICP-15; Normas técnicas da ICP-Brasil. <i>Uptime</i> do serviço de Validação. Tempo médio de resposta da API de validação.

Matriz RACI

Função RACI	Descrição
R - Responsible	Equipes técnicas (Squads): Governança de Serviços de TIC, Operação de Datacenter, Sustentação de aplicações e banco de dados, Infraestrutura de redes e conectividade, Cibersegurança, Gerenciamento e Execução de Serviços Negociais DITEC. Gerencial: COSES; COTEC; COSEG
A - Accountable	COSES
C - Consulted	Comitê Gestor ICP-Brasil; Auditoria Interna; Órgãos integrados; Entidades ICP-Brasil
I - Informed	Usuários internos; Usuários externos Gov.br; Integradores API; Demais diretorias do ITI

2.4.

S-04 - Serviço de Auditoria e Sincronização de Tempo

ID do Serviço	S-04
Nome do Serviço (Resultado Pretendido)	Serviço de Auditoria e Sincronização de Tempo
Descrição do Serviço e Alinhamento ao ITI	Operação e manutenção dos equipamentos que compõem a Entidade de Auditoria do Tempo (EAT) da ICP-Brasil. Este serviço garante a precisão e confiabilidade temporal, o que é fundamental para a Infraestrutura de Chaves Públicas Brasileira.
Base Normativa de Suporte e outras informações	Requisitos da EAT; Normas ICP-Brasil; Ação ACTI-02 do PDTIC.

Matriz RACI

Função RACI	Descrição
R - Responsible	Equipes técnicas (Squads): Governança de Serviços de TIC, Operação de Datacenter, Sustentação de aplicações e banco de dados, Infraestrutura de redes e conectividade, Cibersegurança, Gerenciamento e Execução de Serviços Negociais DITEC. Gerencial: COICP; COTEC; COSEG; SETEM
A - Accountable	SETEM
C - Consulted	Comitê Gestor ICP-Brasil; Auditoria Interna; Órgãos integrados; Entidades ICP-Brasil
I - Informed	Usuários internos; Usuários externos Gov.br; Integradores API; Demais diretorias do ITI

2.5.

S-05 - Gestão e Publicação da Lista de Confiança

ID do Serviço	S-05
----------------------	-------------

Nome do Serviço (Resultado Pretendido)	Gestão e Publicação da Lista de Confiança
Descrição do Serviço e Alinhamento ao ITI	Serviço que designa o ITI como Operador do Esquema da Lista de Confiança (TLSO) da ICP-Brasil. Envolve a definição, publicação, manutenção e assinatura digital da Lista de Confiança (TL) em formato XML, garantindo a autenticidade e o histórico de <i>status</i> dos Prestadores de Serviço de Confiança (PSCs).
Base Normativa de Suporte e outras informações	Normas ICP-Brasil referentes à TL; Requisitos de Governança ICP-Brasil.

Matriz RACI

Função RACI	Descrição
R - Responsible	Equipes técnicas (Squads): Governança de Serviços de TIC, Operação de Datacenter, Sustentação de aplicações e banco de dados, Infraestrutura de redes e conectividade, Cibersegurança, Gerenciamento e Execução de Serviços Negociais DITEC. Gerencial: COICP; COTEC; COSEG
A - Accountable	COICP
C - Consulted	Comitê Gestor ICP-Brasil; Auditoria Interna; Órgãos integrados; Entidades ICP-Brasil
I - Informed	Integradores API; Demais diretorias do ITI

2.6.

S-06 - Operação da Infraestrutura Tecnológica (Nível 3)

ID do Serviço	S-06
Nome do Serviço (Resultado Pretendido)	Operação da Infraestrutura Tecnológica (Nível 3)
Descrição do Serviço e Alinhamento ao ITI	Operação contínua (24x7x365) da infraestrutura crítica de hardware, conectividade, software e segurança que sustenta AC Raiz e serviços negociais. Resolução de incidentes e problemas de alta complexidade (Nível 3/4) que afetam a infraestrutura especializada e crítica, como redes SAN, servidores de aplicação, <i>firewalls</i> da DITEC. Este serviço assemelha-se ao terceiro nível de atendimento, onde especialistas realizam atividades técnicas preestabelecidas e de reparo/restauro.

Base Normativa de Suporte e outras informações	PDTIC ACTI-13; Normas de segurança e continuidade (ICP-Brasil). Suporte especializado à infraestrutura. Tempo Médio para Resolução (TMR) de Incidentes Críticos, conforme Indicadores de Níveis de Serviços (INS) estabelecidos
---	---

Embora as atividades de Operação de Infraestrutura de TIC (como sustentação, *backup*, monitoramento e gerenciamento operacional) sejam frequentemente classificadas como Serviços Técnicos (ou de Apoio), necessários para o provedor de serviço de TIC entregar serviços voltados ao cliente, o Catálogo de Serviços da DITEC a lista expressamente como um serviço negocial sob a denominação de "Atendimento Especializado em Infraestrutura (Nível 3)".

Este serviço é tipicamente contratado para sustentar ambientes de altíssima criticidade, como o CCD/ITI, onde especialistas da contratada realizam a manutenção periódica e o reparo/restauro de incidentes e problemas, assemelhando-se ao terceiro nível de atendimento. O suporte Nível 3 é uma ação listada no PDTIC como "Serviços especializados de suporte à infraestrutura de datacenter e de redes de dados (Nível 3)" (ACTI-13).

Matriz RACI

Função RACI	Descrição
R - Responsible	Equipes Técnicas (<i>squads</i>): Governança de Serviços de TIC, Operação de Datacenter, Sustentação de aplicações e banco de dados, Infraestrutura de redes e conectividade, Cibersegurança. Gerencial: COTEC; COSEG;
A - Accountable	CGISE
C - Consulted	Comitê Gestor ICP-Brasil; Auditoria Interna; Órgãos integrados; Entidades ICP-Brasil
I - Informed	Usuários internos; Usuários externos Gov.br; Integradores API; Demais diretorias do ITI

2.7. S-07 - Serviços de Inteligência e Análise Preditiva para Auditoria/Fiscalização

ID do Serviço	S-07
Nome do Serviço (Resultado Pretendido)	Serviços de Inteligência e Análise Preditiva para Auditoria/Fiscalização
Descrição do Serviço e Alinhamento ao ITI	Apoio operacional às ferramentas e sistemas usados por DAFN para auditoria e fiscalização da ICP-Brasil.
Base Normativa de Suporte e outras informações	Alinhamento aos DOC ICP 08 e 09 INSTRUÇÃO NORMATIVA ITI Nº 31, DE 14 DE MARÇO DE 2025 INSTRUÇÃO NORMATIVA ITI Nº 32, DE 23 DE ABRIL DE 2025

Matriz RACI

Função RACI	Descrição
R - Responsible	Equipes Técnicas (squads): Governança de Serviços de TIC, Operação de Datacenter, Sustentação de aplicações e banco de dados, Infraestrutura de redes e conectividade, Cibersegurança, Gerenciamento e Execução de Serviços Negociais DITEC, Gerenciamento e Execução de Serviços Negociais DAFN. Gerencial: DAFN
A - Accountable	DAFN
C - Consulted	Comitê Gestor ICP-Brasil; Auditoria Interna; Órgãos integrados; Entidades ICP-Brasil
I - Informed	Usuários internos; Demais diretorias do ITI

2.8.
Brasil

S-08 - Sustentação dos Sistemas de Combate à Fraude da ICP-

ID do Serviço	S-08
Nome do Serviço (Resultado Pretendido)	Sustentação dos Sistemas de Combate à Fraude da ICP-Brasil
Descrição do Serviço e Alinhamento ao ITI	Prover com propriedade o serviço segurança e de tratamento de informações recebidas das entidades da ICP Brasil e disponibilizar informações à sociedade brasileira; Oferecendo p tratamento seguro de informações provenientes das entidades da ICP-Brasil para prevenção e combate a fraude
Base Normativa de Suporte e outras informações	DOC-ICP-05; DOC-ICP-05.02; DOC-ICP-05.03; IN ITI nº 31/2025.

Matriz RACI

Função RACI	Descrição
R - Responsible	Equipes Técnicas (squads): Governança de Serviços de TIC, Operação de Datacenter, Sustentação de aplicações e banco de dados, Infraestrutura de redes e conectividade, Cibersegurança, Gerenciamento e Execução de Serviços Negociais DITEC, Gerenciamento e Execução de Serviços Negociais DAFN. Gerencial: DAFN
A - Accountable	DAFN
C - Consulted	Comitê Gestor ICP-Brasil; Auditoria Interna; Órgãos integrados; Entidades ICP-Brasil
I - Informed	Usuários internos; Demais diretorias do ITI

3. CATÁLOGO DE SERVIÇOS TÉCNICOS

Este catálogo detalha os **Serviços de Tecnologia da Informação e Comunicação (TIC)** e atividades operacionais necessárias para suportar os Serviços Negociais. Estas atividades estão agrupadas em:

- I - **Natureza do Serviço:** Definição de áreas de atuação. Uma subdivisão do ecossistema de Tecnologia da Informação e Comunicação (TIC) construída com base na Portaria SGD/MGI nº 1.070/2023 e ABNT NBR ISO/IEC 20000:2020.
- II - **Grupos:** Subdivisão da "Natureza do Serviço", possui um GRUPO-ID.
- III - **Serviços:** Subdivisão de "Grupos", possui um SERV-ID.
- IV - **Atividades Operacionais:** Práticas e procedimentos aplicáveis para atingir o resultado esperado em cada "Serviço", pode ser identificado com um ATV-ID.

A ABNT NBR ISO/IEC 20000-1:2020 estabelece os requisitos para um Sistema de Gestão de Serviço (SGS), focando no planejamento, desenho, transição, entrega e melhoria contínua de serviços para entregar valor e atender aos requisitos de serviço.

A descrição de cada Categoria Operacional e de Gestão é alinhada aos requisitos de gestão da ABNT NBR ISO/IEC 20000-1, foram utilizadas para definir a Tabela a seguir.

Quadro resumo de Categorias e Grupos

Seção	Categoria Operacional e de Gestão	GRUPO-ID	Nome do Grupo
3.1	Gerenciamento de Serviços de TIC	GS-01	Gestão de Incidentes Críticos
		GS-02	Gestão de Problemas
		GS-03	Gestão de Mudanças
		GS-04	Manutenção de Base de Conhecimento
3.2	Sustentação de Aplicações	SA-01	Administração de Servidores de Aplicação
		SA-02	Gerenciamento de Plataformas de Virtualização/Containers
		SA-03	Suporte ao Ambiente DevOps/DevSecOps
3.3	Armazenamento e Backup	AB-01	Gerenciamento de Storages e SAN
		AB-02	Execução de Rotinas de Backup e Restauração
		AB-03	Replicação e Continuidade
		DB-01	Administração e Otimização de Banco de Dados

3.4	Banco de Dados		
3.5	Conectividade e Comunicação	DB-02	Suporte a ETL
		DB-03	Segurança de Dados Críticos
		CC-01	Administração de Ativos de Rede
		CC-02	Gerenciamento de Redes Lógicas
3.6	Segurança de TIC	CC-03	Suporte a Links e Interconexão (WAN/VPN)
		SG-01	Operação do SOC (Security Operations Center)
		SG-02	Gerenciamento de Segurança de Perímetro
		SG-03	Gestão de Credenciais e Acessos
3.7	Monitoramento de Serviços de TI	SG-04	Tratamento de Vulnerabilidades
		MT-01	Operação do NOC (Network Operations Center)
		MT-02	Geração de Relatórios de Desempenho:
		MT-03	Monitoramento do Ambiente Seguro
3.8	Suporte Técnico de Microinformática	ST-01	Gerenciamento de Chamados
		ST-02	Gestão de Acessos ao E-mail e Compartilhamento

Matriz de Mapeamento Categorias de Serviços de TIC e Serviços Negociais

	S-01	S-02	S-03	S-04	S-05	S-06	S-07	S-08
GS	X	X	X	X	X	X	X	X
SA	X	X	X	-	X	X	X	X
AB	X	X	X	X	X	X	X	X
DB	X	X	X	X	X	X	X	X
CC	X	X	X	X	X	X	X	X
SG	X	X	X	X	X	X	X	X
MT	X	X	X	X	X	X	X	X
ST	X	X	X	X	X	X	X	X

3.1. Gerenciamento de Serviços de TIC (GS)

O Gerenciamento de Serviços de TIC representa o próprio Sistema de Gestão de Serviço (SGS).

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: Busca a estabilidade e previsibilidade dos processos através da implantação, manutenção e atualização dos processos de GSTI definidos pelo contratante, baseados nas melhores práticas. Isso inclui adaptar os fluxos básicos de incidentes, requisição, mudanças, problemas e configuração, utilizando ferramenta(s) especializada(s).

Atividades de coordenação e gestão de processos, utilizando ferramentas de Gerenciamento de Serviços de TIC (*ITSM*).

GRUPO-ID	Nome do Grupo	Descrição do Grupo
GS-01	Gestão de Incidentes Críticos	Classificação, registro, e encaminhamento de falhas que impactam a AC Raiz ou Assinaturas Avançadas (em regime 24x7x365)
GS-02	Gestão de Problemas	Investigação de causa raiz de incidentes recorrentes
GS-03	Gestão de Mudanças	Proposição, avaliação e execução de mudanças na infraestrutura de TIC (servidores, <i>firewalls</i> , redes), com foco na segurança integrada e nos processos de DevSecOps
GS-04	Manutenção de Base de Conhecimento	Criação e atualização de procedimentos operacionais, relatórios e documentação técnica

3.1.1.1. **GS-01 - Gestão de Incidentes Críticos**

ID-GRUPO	GS-01
Objetivo do Grupo de Serviços	Restaurar serviços críticos com rapidez, reduzir impacto e garantir comunicação clara.
Equipes Técnicas (Squads)	Governança de Serviços de TIC (Squad GS)
Período de Atendimento	NOC 24x7; Pós-incidente 8x5
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
GS01.01	Acionamento e Comunicação de Crises	Garantir a notificação e comunicação claras durante incidentes de alta prioridade.	Não	Alta
GS01.02	Restauração Emergencial de Serviços (Workaround)	Aplicar soluções de contorno para restaurar a funcionalidade operacional do serviço rapidamente.	Não	Alta

GS01.03	Análise Pós-Incidente e Registro de Lições Aprendidas	Documentar a falha e registrar lições para melhoria contínua dos processos de TIC.	Não	Média

3.1.2. GS-02 - Gestão de Problemas

ID-GRUPO	GS-02
Objetivo do Grupo de Serviços	Identificar causa-raiz e prevenir recorrência, mantendo KEDB.
Equipes Técnicas (Squads)	Governança de Serviços de TIC (Squad GS)
Período de Atendimento	8x5
Necessita Aprovação?	Não
Criticidade	Média

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
GS02.01	Identificação Proativa e Reativa de Problemas	Analisar tendências de incidentes para identificar a causa-raiz (problema) subjacente.	Não	Média
GS02.02	Diagnóstico de Causa-Raiz (RCA) e Mitigação	Investigar e determinar a causa fundamental do problema, elaborando recomendações de solução definitiva.	Não	Média
GS02.03	Gerenciamento de Erros Conhecidos e Soluções Definitivas	Manter um registro de erros conhecidos e acompanhar a implementação das mudanças que eliminam o problema.	Sim	Média

3.1.3. GS-03 - Gestão de Mudanças

ID-GRUPO	GS-03
Objetivo do Grupo de Serviços	Controlar riscos, janelas, rollback e aprovar intervenções.
Equipes Técnicas (Squads)	Governança de Serviços de TIC (Squad GS)
Período de Atendimento	8x5 + janelas noturnas
Necessita Aprovação?	Sim
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
GS03.01	Gestão do Processo de Mudanças e Risco (Registro, Avaliação e Aprovação)	Garantir que o risco das alterações seja avaliado, documentado e aprovado antes da execução.	Sim	Alta

GS03.02	Execução, Planejamento e Coordenação da Mudança	Planejar, coordenar o desenvolvimento/implantação e avaliar os resultados da intervenção física ou lógica.	Sim	Alta

3.1.4. **GS-04 - Manutenção de Base de Conhecimento**

ID-GRUPO	GS-04
Objetivo do Grupo de Serviços	Padronizar soluções e reduzir MTTR.
Equipes Técnicas (Squads)	Governança de Serviços de TIC (Squad GS)
Período de Atendimento	8x5
Necessita Aprovação?	Não
Criticidade	Média

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
GS04.01	Criação e Manutenção de Manuais Técnicos e Operacionais	Manter a documentação de referência para instalação, configuração e operação de sistemas (incluindo Linux/OpenBSD).	Não	Baixa
GS04.02	Manutenção da Documentação de Processos (Auditoria e Solução de Problemas)	Documentar o processo de auditoria e manter o registro de solução de problemas conhecidos.	Não	Baixa
GS04.03	Atualização de Registros Técnicos, Políticas e Recomendações	Manter atualizadas as políticas, recomendações e registros técnicos diversos.	Não	Baixa

3.2. **Sustentação de Aplicações (SA)**

A Sustentação de Aplicações (ou Sustentação de Infraestrutura para Aplicações) refere-se à operação e manutenção da **camada de sustentação de serviços e aplicações** do contratante.

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: Relaciona-se ao Gerenciamento de Incidentes, Problemas, Requisições e Mudanças. As atividades envolvem projetar, operar, administrar e manter os servidores físicos e virtuais, e realizar configurações, alterações e otimizações no ambiente, garantindo que o ambiente seja mantido atualizado observando as orientações previstas no gerenciamento de mudanças. É uma categoria que pode ser indicada para ambientes com abordagens DevOps ou DevSecOps.

Operação e manutenção da camada tecnológica que suporta os serviços finalísticos (excluindo o desenvolvimento de *software* próprio).

Relaciona-se ao Gerenciamento de Incidentes, Problemas, Requisições e Mudanças. As atividades envolvem projetar, operar, administrar e manter os

servidores físicos e virtuais, e realizar configurações, alterações e otimizações no ambiente, garantindo que o ambiente seja mantido atualizado observando as orientações previstas no gerenciamento de mudanças. É uma categoria que pode ser indicada para ambientes com abordagens DevOps ou DevSecOps.

Operação e manutenção da camada tecnológica que suporta os serviços finalísticos (excluindo o desenvolvimento de *software* próprio).

GRUPO-ID	Nome do Grupo	Descrição do Grupo
SA-01	Administração de Servidores de Aplicação	Sustentação de servidores <i>web</i> e <i>proxy</i> , incluindo instalação, configuração e manutenção
SA-02	Gerenciamento de Plataformas de Virtualização/Containers	Operação e suporte de plataformas de virtualização e gerenciamento de infraestrutura em <i>containers</i> (orquestração e automação)
SA-03	Suporte ao Ambiente DevOps/DevSecOps	Gestão de ferramentas e ambientes de Integração Contínua/Testes Contínuos (CI/CD) e controle de versão, conforme a abordagem metodológica adotada

3.2.1. SA-01: Administração de Servidores de Aplicação

ID-GRUPO	SA-01
Objetivo do Grupo de Serviços	Manter aplicações críticas com estabilidade, desempenho e segurança.
Equipes Técnicas (Squads)	Sustentação de Aplicações (Squad SA)
Período de Atendimento	8x5 + janelas
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
SA01.01	Administração e Troubleshooting (solução de problemas) de Aplicações Críticas	Gerenciar a sustentação, recursos e solução de problemas de aplicações negócias.	Não	Alta
SA01.02	Gestão de Configurações de DNS e Serviços Web	Gerenciar entradas DNS (interno/externo), mudar configurações do serviço DNS e de Servidor Web.	Não	Média

SA01.03	Configuração e Renovação de Certificados (Lets Encrypt)	Garantir a segurança das comunicações por meio da emissão e renovação de certificados SSL/TLS.	Não	Alta
SA01.04	Sustentação e Configuração de Serviços de Diretório	Instalar, configurar e alterar políticas do serviço de diretório e sua autenticação em aplicações Web.	Não	Média
SA01.05	Implantação e Atualização de Aplicações e Microserviços	Realizar a instalação, configuração e atualização de aplicações específicas e de microserviços.	Não	Média
SA01.06	Avaliação de Procedimentos de Contingência e Recuperação de Desastres	Validar a efetividade dos planos de continuidade para aplicações.	Não	Alta

3.2.2. SA-02 - Gerenciamento de Plataformas de Virtualização/Containers

ID-GRUPO	SA-02
Objetivo do Grupo de Serviços	Gerenciar VMs, clusters e automação IaC.
Equipes Técnicas (Squads)	Sustentação de Aplicações (Squad SA)
Período de Atendimento	8x5 + janelas
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
SA02.01	Gestão do Ciclo de Vida de VMs e Hosts (Criação, Migração e Recursos)	Criar, migrar, excluir e recuperar VMs, gerenciar recursos (CPU/RAM/IOPS) e expansão de datastores/discos.	Não	Média
SA02.02	Administração da Imagem Padrão (Templates e Cloud-init)	Criar, clonar e gerenciar templates e arquivos de configuração (Cloud-init) para automatizar a criação de VMs.	Não	Média
SA02.03	Sustentação e Hardening de SO em Plataformas (Instalação e Configuração)	Instalar, configurar e aplicar <i>hardening</i> em Sistemas Operacionais para servidores de aplicação.	Não	Média
SA02.04	Gestão e Sustentação de Clusters Kubernetes (K8s)	Instalar, renovar certificados e realizar <i>troubleshooting</i> em serviços de clusters de Kubernetes.	Não	Alta

SA02.05	Administração de Plataformas de Log e Segurança (Graylog, Wazuh, Opensearch)	Instalar, configurar e gerenciar clusters e <i>inputs</i> /agentes de sistemas de Logs (Graylog, Opensearch) e EDR (Wazuh).	Não	Média
SA02.06	Implantação e Manutenção do Console de Virtualização (vCenter)	Instalar e aplicar patches/atualizações no console de gerenciamento de virtualização (VMware vCenter).	Não	Média

3.2.3. SA-03 - Suporte ao Ambiente DevOps/DevSecOps

ID-GRUPO	SA-03
Objetivo do Grupo de Serviços	Operar pipelines, CI/CD e SRE/SLO.
Equipes Técnicas (Squads)	Sustentação de Aplicações (Squad SA)
Período de Atendimento	8x5
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
SA03.01	Gestão do Repositório de Artefatos (Nexus) e Pipeline	Administrar repositórios (locais, remotos), acessos, automação de upload/download e limpeza de artefatos (Nexus).	Não	Média
SA03.02	Suporte e Sustentação do Ambiente de Entrega Contínua (ArgoCD/Gitlab)	Administrar projetos, sincronização, RBAC e execuções de <i>rollback</i> automático/manual em Ambiente de Entrega Contínua	Não	Média
SA03.03	Gerenciamento e Automação de Código e Ambientes	Administrar permissões e versionamento de código-fonte, criar ambientes sob demanda e desenvolver <i>scripts</i> (Python/Bash) e <i>playbooks</i> (Ansible).	Não	Média
SA03.04	Integração Contínua e Build de Imagens (CI/CD)	Gerir a integração e entrega contínua, automatizar rotinas de validação e <i>build</i> de Imagens Docker.	Não	Média
SA03.05	Garantia de Segurança e Disponibilidade do Ecossistema DevOps	Assegurar a compatibilidade e segurança dos ambientes, e avaliar indisponibilidade de aplicações/APIs.	Não	Alta

3.3. Armazenamento e Backup (AB)

Esta categoria abrange o suporte e a operação do ambiente de cópias de segurança e persistência de dados.

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: É essencial para garantir a Disponibilidade do serviço e a Continuidade de Negócios (ABNT NBR 22301 é uma norma relacionada). Envolve a execução de rotinas, restauração e checagem dos backups, e a realização de testes de *restore* com definição de frequência. O gerenciamento do *Storage* envolve a instalação, configuração, otimização, criação, realocação e restauração de sistemas de arquivos. Está também ligada ao Gerenciamento de Ativo.

Gestão da camada de dados para garantir a integridade e recuperação.

GRUPO-ID	Nome do Grupo	Descrição do Grupo
AB-01	Gerenciamento de Storages e SAN	Administração, realocação e restauração de sistemas de arquivos em <i>Storages</i> e <i>Switches</i> SAN
AB-02	Execução de Rotinas de Backup e Restauração	Operação da solução de <i>backup</i> (incluindo Tape Library) e execução de rotinas programadas de <i>backup</i> e <i>restore</i> de banco de dados e sistemas
AB-03	Replicação e Continuidade	Operação dos mecanismos de replicação de dados entre os sítios de redundância, essenciais para a Continuidade do Serviço (capacidade de entregar serviço sem interrupção)

3.3.1. AB-01: Gerenciamento de Storages e SAN

ID-GRUPO	AB-01
Objetivo do Grupo de Serviços	Gerenciar capacidade, IOPS, LUNs e datastores.
Equipes Técnicas (Squads)	Datacenter / Armazenamento (Squad AB)
Período de Atendimento	8x5 + janelas
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
AB01.01	Gestão de Capacidade e Desempenho (I/O)	Gerenciar alocação de espaço, quotas e acompanhar métricas de I/O do storage.	Não	Média
AB01.02	Criação e Configuração de LUNs (logical unit number) e Datastores	Configurar volumes de armazenamento utilizando os protocolos (NFS, ISCSI, Fibre Channel) para hosts.	Não	Média

AB01.03	Manutenção Física e Lógica do Storage	Executar a manutenção periódica para garantir a saúde e o funcionamento correto do equipamento.	Não	Alta
AB01.04	Administração de Hosts de Armazenamento e Virtualização	Administrar hosts ESXI e vCenter ligados ao ambiente de armazenamento.	Não	Média

3.3.2. AB-02: Execução de Rotinas de Backup e Restauração

ID-GRUPO	AB-02
Objetivo do Grupo de Serviços	Garantir backups $\geq 98\%$ e restore de prova.
Equipes Técnicas (Squads)	Datacenter / Armazenamento (Squad AB)
Período de Atendimento	8x5 (monitoramento diário)
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
AB02.01	Monitoramento e Sustentação Diária de Jobs de Backup	Monitorar diariamente, automatizar alertas de falhas e ajustar janelas de Jobs Veeam e demais rotinas de cópia de segurança.	Não	Alta
AB02.02	Gestão do Software de Backup (Veeam) e Mídia Física	Configurar jobs (full, incremental, diferencial), gerenciar fitas de backup e manter o servidor Veeam atualizado.	Não	Média
AB02.03	Serviço de Restauração On-Demand e Recuperação de Sistemas	Executar a restauração de arquivos individuais, VMs completas e configurações críticas, garantindo a recuperação em caso de falhas.	Não	Alta
AB02.04	Validação e Confirmação da Integridade dos Backups	Validar a integridade das cópias de segurança (bancos, logs, arquivos, repositórios) e garantir sua consistência.	Não	Alta

3.3.3. AB-03: Replicação e Continuidade

ID-GRUPO	AB-03
Objetivo do Grupo de Serviços	Realizar replicação contínua e testes DR.
Equipes Técnicas (Squads)	Datacenter / Armazenamento (Squad AB)

Período de Atendimento	8x5 + janelas
Necessita Aprovação?	Sim
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
AB03.01	Configuração e Manutenção de Rotinas de Replicação	Estabelecer a replicação contínua de dados e sistemas entre sítios de contingência (DR).	Não	Alta
AB03.02	Testes de Recuperação de Desastres (DR Test)	Executar simulações periódicas do plano de DR para validar a capacidade de restauração e os tempos de RTO e RPO.	Não	Alta
AB03.03	Gestão de Infraestrutura e Documentação do Sítio de Contingência	Administrar e manter a infraestrutura do ambiente DR e atualizar estratégias e procedimentos de continuidade.	Não	Média

3.4. **Sustentação de Banco de Dados e Administração de Dados (DB)**

Foca na operação e suporte dos Sistemas Gerenciadores de Banco de Dados (SGBD) e seus recursos relacionados.

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: As atividades de sustentação (projetar, instalar, implantar, operar, administrar e manter) devem garantir a otimização de desempenho e o Gerenciamento de Incidentes, Problemas, Requisições e Mudanças relacionados ao ambiente de banco de dados. O perfil profissional responsável por isso também atua no monitoramento dos recursos de banco de dados.

Esta categoria também trata da governança, modelagem e manipulação estratégica dos dados.

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: Está ligada à Gestão de Configuração (relacionamento de ICs) e à Gestão de Riscos. Inclui apoiar a auditoria, análise, revisão de documentação relativas à modelagem de dados e a manutenção de repositório de metadados. Também engloba Apoio na elaboração e definição de política de segurança do banco de dados e o Desenvolvimento, execução, teste e documentação de rotinas de Extração, Transformação e Carga - ETL.

Gerenciamento dos recursos de dados transacionais e analíticos.

GRUPO-ID	Nome do Grupo	Descrição do Grupo
DB-01	Administração e Otimização de Banco de Dados	Operação, gerenciamento, otimização, e monitoramento dos recursos de banco de dados transacionais e analíticos

DB-02	Suporte a ETL	Operação e sustentação de ferramentas de Extração, Transformação e Carga (ETL) e apoio à administração de dados
DB-03	Segurança de Dados Críticos	Implementação de políticas de acesso, <i>hardening</i> e <i>patch management</i> para os bancos de dados que armazenam informações sensíveis da ICP-Brasil

3.4.1. DB-01: Administração e Otimização de Banco de Dados

ID-GRUPO	DB-01
Objetivo do Grupo de Serviços	Otimizar performance, HA, tuning e monitoramento.
Equipes Técnicas (Squads)	Banco de Dados (Squad DB)
Período de Atendimento	8x5
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
DB01.01	Sustentação e Otimização de Performance de SGBD	Ajustar parâmetros, otimizar consultas e estrutura lógica, e gerenciar recursos para eliminar gargalos (CPU, memória, I/O).	Não	Média
DB01.02	Implantação e Manutenção do SGBD	Instalar, configurar e gerenciar versões/patches de segurança de SGBDs (PostgreSQL, MySQL, etc.).	Não	Média
DB01.03	Gestão de Alta Disponibilidade (HA) e Recovery	Configurar replicação, <i>clustering</i> , <i>log shipping</i> e implementar soluções de <i>failover</i> e <i>recovery</i> para garantir a disponibilidade.	Não	Alta
DB01.04	Monitoramento e Correção de Falhas e Inconsistências	Monitorar conexões ativas, sessões e <i>locks</i> , e detectar/corrigir falhas e inconsistências para manter a saúde do banco.	Não	Alta
DB01.05	Gerenciamento de Espaço e Recursos Físicos	Gerir <i>tablespaces</i> , arquivos de log e diretórios de dados.	Não	Média

3.4.2. DB-02 - Suporte a ETL

ID-GRUPO	DB-02
Objetivo do Grupo de Serviços	Gerenciar fluxos ETL e integrações.

Equipes Técnicas (Squads)	Banco de Dados / Dados (Squad DB)
Período de Atendimento	8x5
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
DB02.01	Suporte e Otimização de Jobs de ETL	Oferecer suporte para garantir a execução, performance e integridade dos processos de Extração, Transformação e Carga (ETL).	Não	Média
DB02.02	Monitoramento de Fluxos de Dados e Cargas	Acompanhar a execução e o desempenho dos processos de ETL, identificando e corrigindo falhas nas cargas de dados.	Não	Média
DB02.03	Configuração de Conectividade e Fontes de Dados	Gerenciar e configurar as conexões necessárias para que os processos de ETL acessem as fontes e destinos de dados.	Não	Média

3.4.3. DB-03 - Segurança de Dados Críticos

ID-GRUPO	DB-03
Objetivo do Grupo de Serviços	Aplicar hardening, criptografia e auditorias.
Equipes Técnicas (Squads)	Banco de Dados (Squad DB)
Período de Atendimento	8x5
Necessita Aprovação?	Sim
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
DB03.01	Aplicação de Criptografia e Mascaramento de Dados	Implementar e gerenciar técnicas de criptografia e mascaramento para proteger dados sensíveis em repouso e em trânsito.	Sim	Alta
DB03.02	Auditoria e <i>Hardening</i> de Segurança do SGBD	Executar auditorias de conformidade e aplicar configurações de segurança para mitigar riscos e vulnerabilidades de banco de dados.	Não	Alta
DB03.03	Gerenciamento de Logs de Acesso Crítico ao Banco	Configurar, monitorar e analisar logs de auditoria de acessos privilegiados e de atividades críticas no SGBD.	Não	Alta

3.5. Conectividade e Comunicação (CC)

Concentra-se na operação e manutenção da rede de comunicação de dados e voz.

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: Garante a Disponibilidade dos serviços. As atividades envolvem projetar, operar, administrar e manter o conjunto de soluções de *hardware* e *software* que compõe o ambiente de conectividade e comunicação. Isso inclui realizar configurações, alterações e otimizações no ambiente e manter a documentação atualizada, o que é essencial para o Gerenciamento de Ativos e a Gestão de Configuração.

Operação e sustentação da infraestrutura de rede da DITEC (que possui LAN própria).

GRUPO-ID	Nome do Grupo	Descrição do Grupo
CC-01	Administração de Ativos de Rede	Instalação, manutenção, configuração e remoção de <i>switches</i> , roteadores e outros ativos de rede nos sítios de prestação de serviço (Sala Cofre/CCD)
CC-02	Gerenciamento de Redes Lógicas	Criação, remoção e manutenção de Redes Locais Virtuais (VLANs) e rotas
CC-03	Suporte a Links e Interconexão (WAN/VPN)	Gerenciamento e resolução de incidentes em enlaces de dados de longa distância e serviços de VPN <i>site-to-site</i> (IPv4 e IPv6)

3.5.1. **CC-01 - Administração de Ativos de Rede**

ID-GRUPO	CC-01
Objetivo do Grupo de Serviços	Provisionar equipamentos, firmware, segmentação.
Equipes Técnicas (Squads)	Redes e Conectividade (Squad CC)
Período de Atendimento	12x5 + NOC 24x7
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
CC01.01	Gestão de Configurações de Ativos (CLI/Provisionamento)	Realizar o provisionamento inicial via CLI, configurar interfaces, trunks, remover configurações obsoletas e instalar patches de firmware em switches.	Não	Média
CC01.02	Implantação e Manutenção Física de Ativos (Racks e Servidores)	Realizar o gerenciamento físico dos racks, cabeamento estruturado e a instalação física de Servidor em Rack.	Não	Baixa
CC01.03	Segmentação de Tráfego e Implementação de VLANs/Sub-redes	Segmentar tráfego para desempenho/segurança e implementar/ajustar VLANs e sub-redes.	Não	Média

CC01.04	Administração e Implantação de Ativos de Borda (Switch, Firewall)	Configurar/Instalar Switches, Firewall e aplicações de Firewall NGFW para garantir a conectividade e segurança.	Não	Alta
CC01.05	Administração de Conectividade e Links de Internet	Garantir a disponibilidade, confiabilidade e conectividade entre redes, administrando os links de internet.	Não	Alta
CC01.06	Gestão de Inventário e Documentação da Rede	Realizar inventário dos equipamentos, documentar a topologia física e lógica e atualizar diagramas de conexões.	Não	Média

3.5.2. CC-02 - Gerenciamento de Redes Lógicas

ID-GRUPO	CC-02
Objetivo do Grupo de Serviços	Gerenciar VLANs, rotas e vSwitches.
Equipes Técnicas (Squads)	Redes e Conectividade (Squad CC)
Período de Atendimento	12x5 + NOC 24x7
Necessita Aprovação?	Sim
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
CC02.01	Gestão de Endereçamento IP e Alocação	Controlar o endereçamento IP para evitar conflitos e garantir o uso eficiente dos recursos de rede.	Não	Média
CC02.02	Criação e Mapeamento de Redes Lógicas (vSwitches/VLANs)	Criar vSwitches e VLANs na virtualização e mapear as conexões entre esses segmentos.	Não	Média
CC02.03	Auditoria de Logs de Rede Lógica	Auditar os logs para detectar anomalias no tráfego e acesso da rede local.	Não	Média

3.5.3. CC-03 - Suporte a Links e Interconexão (WAN/VPN)

ID-GRUPO	CC-03
Objetivo do Grupo de Serviços	Garantir enlases, VPN, QoS e redundância.
Equipes Técnicas (Squads)	Redes e Conectividade (Squad CC)
Período de Atendimento	12x5 + NOC 24x7
Necessita Aprovação?	Sim
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
CC03.01	Monitoramento de Desempenho e SLA dos Links	Acompanhar <i>downtime</i> , latência e taxa de utilização (I/O) dos links WAN/LAN, comparando com o SLA.	Não	Alta
CC03.02	Troubleshooting e Teste de Redundância da WAN	Realizar <i>troubleshooting</i> de rede (ping, traceroute), verificar uplinks, erros físicos e testar caminhos redundantes de <i>failover</i> .	Não	Alta
CC03.03	Gestão de Acesso Remoto Seguro (VPN)	Disponibilizar, configurar e gerenciar as conexões VPN para acesso remoto.	Não	Média
CC03.04	Documentação e Rastreabilidade da Interconexão	Atualizar registros, topologia e diagramas de conexões lógicas e físicas, garantindo rastreabilidade.	Não	Média

3.6. Segurança de TIC (SG)

Foca na proteção dos ativos de informação e na gestão dos riscos de segurança.

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: Possibilita a integração com um sistema de gestão da segurança da informação com base na ABNT NBR ISO/IEC 27001. As atividades incluem projetar, operar, administrar e manter o conjunto de soluções (hardwares e softwares) de segurança, tratar incidentes e problemas de segurança, e realizar procedimentos para busca de vulnerabilidades e falhas de segurança no ambiente de TIC. O escopo inclui a configuração de antivírus e a implantação de ambiente de SOC (Security Operations Center).

Operação e monitoramento dos mecanismos de proteção lógica do ambiente, essenciais devido à criticidade da ICP-Brasil e outros serviços.

GRUPO-ID	Nome do Grupo	Descrição do Grupo
SG-01	Operação do SOC (Security Operations Center)	Monitoramento e gerenciamento contínuo (24x7x365) de segurança, incluindo a análise de tentativas de ataque e alertas
SG-02	Gerenciamento de Segurança de Perímetro	Inclusão, alteração e exclusão de regras de <i>firewall</i> (incluindo WAF, IPS/IDS)
SG-03	Gestão de Credenciais e Acessos (IAM)	Criação, modificação, inativação e exclusão de perfis e atributos de contas e senhas para acesso lógico aos sistemas da AC Raiz
SG-04	Tratamento de Vulnerabilidades	Execução de procedimentos para busca e correção de vulnerabilidades e falhas de segurança no ambiente de TIC, incluindo configuração de antivírus

3.6.1. **SG-01 - Operação do SOC (Security Operations Center)**

ID-GRUPO	SG-01
Objetivo do Grupo de Serviços	Operar SIEM/EDR e responder incidentes.
Equipes Técnicas (Squads)	Cibersegurança (Squad SG)
Período de Atendimento	24x7
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
SG01.01	Monitoramento e Detecção de Intrusão/Ameaças (SIEM/EDR)	Monitorar eventos de segurança, detectar intrusão e ameaças EDR em tempo real por meio da análise de logs.	Não	Alta
SG01.02	Tratamento de Artefatos Maliciosos e Resposta a Incidentes	Coordenar e executar a resposta a incidentes (COTIC/COTEC) e realizar o tratamento de artefatos maliciosos.	Não	Alta
SG01.03	Gestão de Inteligência de Ameaças (<i>Threat Intelligence</i>)	Gerenciar e compartilhar informações sobre ameaças e indicadores de comprometimento.	Não	Média

3.6.2. **Gerenciamento de Segurança de Perímetro**

ID-GRUPO	SG-02
Objetivo do Grupo de Serviços	Gerenciar políticas e ataques.
Equipes Técnicas (Squads)	Cibersegurança (Squad SG)
Período de Atendimento	24x7
Necessita Aprovação?	Sim
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
SG02.01	Gestão de Regras e Configurações de Firewall/NGFW	Criar, modificar e remover regras de firewall (incluindo o firewall local do OpenBSD) e gerenciar a higiene das regras.	Sim	Alta
SG02.02	Implantação e Sustentação de Ativos de Segurança (HSM, Antivírus)	Instalar, configurar e atualizar ativos de segurança como o Módulo de Segurança de Hardware (HSM) e ferramentas de Antivírus.	Não	Alta
SG02.03	Gerenciamento de Logs de Acesso Físico (Sala Cofre e Perímetro)	Auditar logs de entradas/saídas da sala cofre e gerenciar o processamento dos registros biométricos.	Não	Alta

SG02.04	Documentação de Controles de Segurança de Perímetro	Documentar os procedimentos e políticas de segurança do perímetro de rede.	Não	Média

3.6.3. SG-03 - Gestão de Acessos

ID-GRUPO	SG-03
Objetivo do Grupo de Serviços	Gerenciar ciclo de vida de credenciais.
Equipes Técnicas (Squads)	Cibersegurança (Squad SG)
Período de Atendimento	8x5 + alertas 24x7
Necessita Aprovação?	Sim
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
SG03.01	Gestão do Ciclo de Vida do Acesso Lógico e Atribuição de Perfis	Registrar novos usuários, gerenciar perfis, atribuir permissões e remover acessos desnecessários.	Não	Média
SG03.02	Revisão e Auditoria de Acessos Privilegiados e Servidores Críticos	Revisar acessos administrativos a <i>switches</i> , <i>firewalls</i> , servidores expostos à Internet e sistemas isolados.	Não	Alta
SG03.03	Validação de Permissões e Conformidade (Lógico e Físico)	Validar permissões de acesso aos sistemas internos/servidores e garantir o alinhamento de funções com acessos lógicos e físicos.	Não	Alta
SG03.04	Gestão de Acessos Físicos e Credenciais (CCD e Áreas Restritas)	Gerenciar cadastros, permissões de acesso físico e atualizar a relação nominal de colaboradores autorizados em áreas críticas.	Não	Alta

3.6.4. SG-04 - Tratamento de Vulnerabilidades

ID-GRUPO	SG-04
Objetivo do Grupo de Serviços	Executar varreduras, correções e priorizações.
Equipes Técnicas (Squads)	Cibersegurança (Squad SG)
Período de Atendimento	24x7 detecção / execução 8x5
Necessita Aprovação?	Não/Sim
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
---------	-----------------	----------------------	---------------------	----------------------

SG04.01	Varredura e Análise de Vulnerabilidades e Riscos	Realizar varredura de vulnerabilidades em sistemas/redes e identificar falhas/riscos em ativos de TIC.	Não	Alta
SG04.02	Tratamento de Vulnerabilidades e Aplicação de Patches	Identificar, classificar, sanar vulnerabilidades e implementar patches de segurança em SOs (Windows, CentOS, OpenBSD).	Não	Alta
SG04.03	Implementação de Controles de Segurança Avançados	Aplicar <i>hardening</i> em sistemas e configurar controles avançados (autenticação MTLS, autenticação multifator, segmentação de rede).	Não	Alta
SG04.04	Auditoria e Conformidade de Acessos e Repositórios	Realizar verificação de conformidade de acessos lógicos e revisar registros de acesso aos repositórios da AC-Raiz.	Não	Alta
SG04.05	Revisão e Auditoria de Controles Físicos e Operacionais	Revisar acessos físicos e validar conformidade das práticas de gestão de pessoal da AC Raiz.	Não	Alta

3.7. Monitoramento de Serviços de TI (MT)

Esta categoria garante a vigilância proativa e a aferição da qualidade dos serviços.

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: É crucial para o monitoramento e a medição dos objetivos de gestão de serviço, e para a medição e avaliação da eficácia dos serviços. Envolve Realizar o monitoramento dos sistemas, aplicações, serviços e infraestrutura de TIC através de ferramenta(s) especializada(s). Também implica em Executar o plano de comunicação realizando os acionamentos dos responsáveis pela resolução, sendo um apoio direto ao Gerenciamento de Incidentes. É indicada para ambientes que possuem central de serviços ou *service desk* implantado.

Atividades que utilizam ferramentas especializadas para monitorar a saúde do ambiente e garantir os Indicadores de Níveis de Serviços (INS).

GRUPO-ID	Nome do Grupo	Descrição do Grupo
MT-01	Operação do NOC (Network Operations Center)	Monitoramento proativo da disponibilidade, <i>performance</i> e uso de recursos da rede, servidores e serviços críticos
MT-02	Geração de Relatórios de Desempenho:	Produção de relatórios automatizados de disponibilidade de Serviços de TIC (medindo INS) e análise de tendências (<i>KPIs</i> da operação).

MT-03	Monitoramento do Ambiente Seguro	Verificação de subsistemas críticos do Centro de Certificação Digital (CCD/ITI), como climatização, CFTV, controle de acesso e alarmes, inclusive por meio de sistemas como o SIGAS (<i>Sistema de Gerenciamento do Ambiente Seguro</i>).

3.7.1. MT-01 - Operação do NOC (Network Operations Center)

ID-GRUPO	MT-01
Objetivo do Grupo de Serviços	Monitorar infraestrutura e serviços 24x7.
Equipes Técnicas (Squads)	Monitoramento (Squad MT)
Período de Atendimento	24x7
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
MT01.01	Administração e Sustentação da Plataforma de Monitoramento (Zabbix)	Atualizar o servidor Zabbix, auditar configurações de agentes e refletir mudanças de infraestrutura nos serviços.	Não	Média
MT01.02	Configuração de Ativos e Alertas no Monitoramento	Adicionar servidores/redes/aplicações, cadastrar hosts e grupos, e configurar <i>triggers/thresholds</i> personalizados (Zabbix).	Não	Média
MT01.03	Gestão de Dashboards e Visualização (Grafana/ArgoCD)	Criar Dashboards (Grafana/Zabbix) e visualizar o <i>status</i> de aplicações via <i>dashboard</i> do ArgoCD.	Não	Baixa
MT01.04	Monitoramento de Certificados Digitais e LCRs	Acompanhar a validade e <i>status</i> de Certificados e Listas de Certificados Revogados (LCRs).	Não	Alta
MT01.05	Gestão e Correlação de Eventos e Notificações	Configurar correlação de eventos, notificações (e-mail, Telegram) e aplicar políticas SNMP traps.	Não	Média
MT01.06	Integração de Ferramentas de Observabilidade (Prometheus/ArgoCD)	Integrar o ArgoCD com ferramentas de monitoramento e configurar o Prometheus para coleta de métricas de aplicações.	Não	Média

3.7.2. MT-02 - Geração de Relatórios de Desempenho

ID-GRUPO	MT-02
Objetivo do Grupo de Serviços	Gerar KPIs e relatórios de Indicadores de Níveis de Serviços (INS).
Equipes Técnicas (Squads)	Monitoramento (Squad MT)
Período de Atendimento	8x5
Necessita Aprovação?	Não
Criticidade	Média

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
MT02.01	Geração de Relatórios e KPIs de Desempenho	Gerar relatórios periódicos de incidentes e KPIs/tendências para planejamento de expansão.	Não	Média
MT02.02	Monitoramento e Relatório de Tráfego e Falhas	Monitorar o tráfego web (filtros), auditar logs de eventos e verificar logs/falhas de backup (Veeam).	Não	Média
MT02.03	Gestão de Indicadores de Disponibilidade	Mensurar <i>uptime</i> e incidentes por serviço e atualizar indicadores de disponibilidade.	Não	Média

3.7.3. MT-03 - Monitoramento do Ambiente Seguro

ID-GRUPO	MT-03
Objetivo do Grupo de Serviços	Acompanhar CFTV, energia, climatização.
Equipes Técnicas (Squads)	Monitoramento (Squad MT)
Período de Atendimento	24x7
Necessita Aprovação?	Não
Criticidade	Alta

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
MT03.01	Monitoramento Contínuo de Sistemas de Segurança Física	Garantir o funcionamento contínuo dos sistemas de segurança física (energia, climatização, controle de acesso).	Não	Alta
MT03.02	Monitoramento e Conformidade de Gravações (CFTV)	Conferir a integridade e disponibilidade das gravações do CFTV, garantindo a retenção conforme política.	Não	Média
MT03.03	Acompanhamento de Manutenção Preventiva e Corretiva	Monitorar as manutenções e intervenções em salas técnicas e no ambiente seguro.	Não	Média

3.8. Suporte Técnico de Microinformática (ST)

Esta categoria compreende o atendimento direto aos usuários.

Atuação segundo a ABNT NBR ISO/IEC 20000-1:2020: Embora seja um serviço de atendimento, ele é o principal mecanismo para os processos de Gerenciamento de Requisição e Gerenciamento de Incidentes. Envolve a prestação de serviços de suporte técnico de microinformática, incluindo a sustentação dos ativos e dos *softwares* relacionados às atividades dos usuários. É o ponto de contato inicial para o registro, classificação, priorização e resolução de incidentes.

Atendimento a usuários internos (servidores e colaboradores) da DITEC.

GRUPO-ID	Nome do Grupo	Descrição do Grupo
ST-01	Gerenciamento de Chamados (Service Desk Nível 1/2)	Registro e resolução de requisições de suporte para usuários corporativos (relacionadas a <i>hardware</i> e <i>software</i> de estação de trabalho)
ST-02	Gestão de Acessos ao E-mail e Compartilhamento	Criação, manutenção e restrição de permissões de acesso ao correio eletrônico e repositórios de compartilhamento de arquivos

3.8.1. ST-01 - Gerenciamento de Chamados (Service Desk Nível 1/2)

ID-GRUPO	ST-01
Objetivo do Grupo de Serviços	Registrar, tratar e encaminhar incidentes de usuários.
Equipes Técnicas (Squads)	Suporte Técnico (Squad ST)
Período de Atendimento	8x5
Necessita Aprovação?	Não
Criticidade	Média

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
ST01.01	Suporte e Onboarding de Estação de Trabalho	Instalação da estação de trabalho, instalação do SO Usuário e configuração de rede na estação de trabalho.	Não	Baixa
ST01.02	Instalação e Configuração de Software Específico e Periféricos	Instalar e configurar impressora, instalar Hardware Criptográfico e instalar/aplicar patches em softwares específicos (SGC, Knet Manager).	Não	Média
ST01.03	Suporte ao Portal e Conferência de Links Públicos	Conferir links e referências públicas no portal do ITI, assegurando acessibilidade e atualização.	Não	Baixa

3.8.2. ST-02: Gestão de Acessos ao E-mail e Compartilhamento

ID-GRUPO	ST-02
Objetivo do Grupo de Serviços	Gerenciar e-mail e permissões.

Equipes Técnicas (Squads)	Suporte Técnico (Squad ST)
Período de Atendimento	8x5
Necessita Aprovação?	Sim
Criticidade	Média

ID-SERV	Nome do Serviço	Objetivos do Serviço	Necessita Aprovação	Nível de Criticidade
ST02.01	Gerenciamento de Contas de E-mail	Gerenciar contas de e-mail em serviços próprios (criação, manutenção, exclusão).	Não	Média
ST02.02	Criação e Configuração de Serviço de Compartilhamento	Criar e configurar Serviço de compartilhamento de arquivo (NFS/SFTP).	Não	Média
ST02.03	Gestão de Acesso a Compartilhamento de Arquivos	Gerenciar as permissões de acesso ao compartilhamento de arquivos.	Não	Média

4. **LISTA DE PARTES INTERESSADAS E APROVADORES**

I - Operacional

a) Categorias de Serviços (ABNT NBR ISO/IEC 20000-1:2020 e Portaria SGD/MGI nº 1.070)

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

b) Equipes Técnicas DITEC (squads)

- Governança de Serviços de TIC
- Operação de Datacenter
- Sustentação de Aplicações e Banco de Dados
- Infraestrutura de Redes e Conectividade
- Cibersegurança
- Gerenciamento e Execução de Serviços Negociais DITEC
- Gerenciamento e Execução de Serviços Negociais DAFN
- Suporte Técnico para Serviços Negociais

c) Profissionais Terceirizados

- Analista de Qualidade, Processos e Serviços de TIC

- Analista de Infraestrutura
- Administrador Plataformas
- Analista DevOps
- Analista de Banco de Dados
- Administrador de Banco de Dados
- Analista NOC 24x7 N2
- Analista NOC 24x7 N3
- Analista SOC 24x7 N1
- Analista SOC 24x7 N2
- Analista SOC 24x7 N3
- Analista de Integração e Testes de Software
- Analista em Segurança e Operações de Serviços
- Analista de Segurança de Dados
- Analista de Auditoria e Conformidade
- Service Desk N1

II - Interessados/Responsáveis

a) Institucionais Internos

- Diretor-Presidente
- DITEC; CGOPE; CGISE; COICP; COSES; COTEC; COSEG, SETEM
- CGICP;
- DAFN;
- DITI;
- DPOA; CGTIC; COTIC
- CGE
- CGDSI
- ETIR
- Encarregado de Dados
- Gestor de Segurança da Informação do ITI
- Comitê de Mudanças da DITEC
- Gestor do Serviço (para cada Serviço Negocial)

b) Interessados - Institucionais Externos

- Comitê Gestor da ICP-Brasil;
- Entidades ICP-Brasil (AC/AR/PSCs);
- Órgãos APF; SGD/MGI
- Entes integrados via API;
- Auditoria;
- Fornecedores;
- Usuários internos
- Usuários externos (cidadão).

5. CONSIDERAÇÕES FINAIS

A ABNT NBR ISO/IEC 20000-1:2020 estabelece os requisitos para um Sistema de Gestão de Serviço (SGS), focando no planejamento, desenho, transição, entrega e melhoria contínua de serviços para entregar valor e atender aos requisitos de serviço. O modelo de contratação de operação de infraestrutura de TIC segue a série ABNT NBR ISO/IEC 20000-1:2020.



Documento assinado eletronicamente por **Rafael de Lima Ramos, Coordenador(a)**, em 01/09/2026, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Alysson Marques, Coordenador-Geral**, em 01/09/2026, às 11:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.it.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0810873** e o código CRC **9C3F92AC**.

Referência: Processo nº 00100.002198/2025-02

SEI nº 0810873

LICITAÇÃO: ANEXO Nº ETP 6/2026 - APÊNDICE III -/2026/ASSESSOR-DITEC/DITEC

Processo nº 00100.002198/2025-02

Interessado: CGISE

APÊNDICE III - EQUIPES TÉCNICAS - DEFINIÇÃO E ATIVIDADES

Lista de Siglas

DR – Disaster Recovery – Recuperação de Desastre
EDR – Endpoint Detection and Response – Detecção e Resposta em Endpoint
GSTI – Gerenciamento de Serviços de Tecnologia da Informação
IPS – Intrusion Prevention System – Sistema de Prevenção de Intrusão
ITSM – Information Technology Service Management – Gerenciamento de Serviços de Tecnologia da Informação
KB – Knowledge Base – Base de Conhecimento
KEDB – Known Error DataBase – Base de Erro Conhecido
NOC – Network Operations Center – Centro de Operações de Rede
NGFW – Next-Generation Firewall – Firewall de Próxima Geração
RPO – Recovery Point Objective – Objetivo de Ponto de Recuperação
RTO – Recovery Time Objective – Objetivo de Tempo de Recuperação
SIEM – Security Information and Event Management – Sistema de Gerenciamento de Informações e Eventos de Segurança
SLO – Service Level Objective – Objetivo de Nível de Serviço
SOC – Security Operations Center – Centro de Operações de Segurança
WAF – Web Application Firewall – Firewall de Aplicação Web

1. DISPOSIÇÕES PRELIMINARES

Este documento detalha as tarefas e atividades da contratação de serviços técnicos especializados de operação e sustentação de infraestrutura de TIC e atendimento à usuários, em conformidade com o modelo de contratação por valor fixo mensal atrelado a Indicadores de Níveis de Serviços (INS) e seus respectivos Níveis Mínimos de Serviço (NMS), conforme Portaria SGD/MGI nº 1.070/2023, e suas atualizações.

O escopo abrange a prestação de serviços continuados para monitoramento e sustentação do ambiente computacional. Estes serviços são voltados para garantir a disponibilidade, integridade, resiliência e segurança dos recursos tecnológicos que suportam a ICP-Brasil e outros Serviços Negociais, que são infraestruturas de missão crítica que não admitem interrupções.

O detalhamento é não exaustivo; a Contratada deverá realizar todas as ações necessárias à adequada execução, observando os processos de GSTI (ITSM), o Catálogo de Serviços e os INS definidos.

1.1. Equipes Técnicas

A partir do que define Portaria SGD/MGI nº 1.070/2023, estabelecendo nove categorias de serviços para Operação de Infraestrutura e Atendimento a Usuários, foram definidas as Equipes Técnicas (squads). De forma a alinhar as categorias de serviços, seus grupos e os próprios serviços ao cotidiano gerencial, como mostra a Tabela 01 a seguir.

Tabela 01. Relação entre Esquipes Técnicas e Categorias de Serviços

#	Equipes Técnicas (squads)	CATEGORIA DE SERVIÇOS (2.3.2 - ANEXO I - Portaria SGD/MGI nº 1.070/2023)
I	Governança de Serviços de TIC	a) Gerenciamento de Serviços de TIC. i) Suporte Técnico de Microinformática.
II	Operação de datacenter	a) Gerenciamento de Serviços de TIC; c) Armazenamento e Backup; h) Monitoramento de Serviços de TI.
II	Sustentação de aplicações e banco de dados	b) Sustentação de Aplicações; d) Sustentação de Banco de Dados; e) Administração de Dados; h) Monitoramento de Serviços de TI.
IV	Infraestrutura de redes e conectividade	f) Conectividade e Comunicação.
V	Cibersegurança	g) Segurança de TIC.
VI	Gerenciamento e execução de serviços negociais DITEC	b) Sustentação de Aplicações; h) Monitoramento de Serviços de TI.
VII	Gerenciamento e execução de serviços negociais DAFN	b) Sustentação de Aplicações; d) Sustentação de Banco de Dados; e) Administração de Dados; h) Monitoramento de Serviços de TI.

A seguir, na tabela 02, relaciona os profissionais demandados para cada Equipe Técnica, com os respectivos níveis de senioridade e quantidades.

Tabela 02. Composição das Esquipes Técnicas/ Squads

#	Equipes Técnicas (squads)	Profissionais	Senioridade	Quantidade
I	Governança de Serviços de TIC	Analista de Serviços de TIC	Junior	2
		Analista de Serviços de TIC	Pleno	1
		Analista de Serviços de TIC	Sênior	1
II	Operação de datacenter	Analista de Infraestrutura	Pleno	3
		Analista de Infraestrutura	Sênior	1
II	Sustentação de aplicações e banco de dados	Administrador Plataformas	Pleno	1
		Administrador Plataformas	Sênior	1
		Analista DevOps	Pleno	2
		Analista de Banco de Dados	Pleno	1
		Administrador de Banco de Dados	Sênior	1
IV	Infraestrutura de redes e conectividade	Analista NOC N2	Pleno	1
		Analista NOC N3	Sênior	1
V	Cibersegurança	Analista SOC N1	Junior	4
		Analista SOC N2	Pleno	4
		Analista SOC N3	Sênior	2
VI	Gerenciamento e execução de serviços comerciais DITEC	Analista de Integração e Testes de Software	Pleno	1
		Analista em Segurança e Operações de Serviços	Pleno	2
VII	Gerenciamento e execução de serviços comerciais DAFN	Analista de Sistemas de Automação	Pleno	2
		Administrador de Dados	Sênior	1
		Analista de Segurança de Dados	Junior	1
		Analista de Auditoria e Conformidade	Pleno	1

Já a Tabela 02 a seguir apresenta detalhes sobre a atuação das Equipes Técnicas no que diz respeito a parâmetros de atuação.

Tabela 03. Informações complementares das Esquipes Técnicas/ Squads

#	Equipes Técnicas (squads)	Janela Padrão	Carga-horária	Regime	Sobre aviso	Potencial para hora extra
I	Governança de Serviços de TIC	09:00 às 18:00 horas	8 h x 5 dias	Presencial	n/a	Baixo, em fechamento de indicadores e inspeções
II	Operação de datacenter	09:00 às 18:00 horas	8 h x 5 dias	Presencial	Cobertura 24x7 - sobreaviso	Alto, concentrado em realização de cerimônias e manutenções no CCD, janelas de atualização e contingências
II	Sustentação de aplicações e banco de dados	09:00 às 18:00 horas	8 h x 5 dias	Presencial	n/a	Médio, em deploys/hotfix e correções urgentes
IV	Infraestrutura de redes e conectividade	09:00 às 18:00 horas	8 h x 5 dias	Presencial	Cobertura 24x7 - sobreaviso	Médio, em deploys/hotfix e correções urgentes
V	Cibersegurança	09:00 às 18:00 horas (presencial)	24 h x 7 dias	Híbrido	n/a	Baixo, dada o squad ser 24x7
VI	Gerenciamento e execução de serviços comerciais DITEC	09:00 às 18:00 horas	8 h x 5 dias	Presencial	n/a	Alto, concentrado em janelas de atualização e contingências
VII	Gerenciamento e execução de serviços comerciais DAFN	09:00 às 18:00 horas	8 h x 5 dias	Presencial	n/a	Médio, concentrado em realização de auditorias e contingências

Cada uma das categorias de serviços será responsável por atuar em um determinado segmento da cadeia de prestação de serviços, de acordo com a sua especialidade e as necessidades das Unidades Organizacionais (UOs) do ITI, de modo a garantir a observância dos níveis de serviço e desempenho estabelecidos.

1.2. Perfis Profissionais de Referência

Para compor a Tabela 02 apresentada anteriormente, os profissionais alocados em cada uma das Equipes técnicas, as habilidades e competências necessárias foram identificadas nos seguintes perfis profissionais de referência, a partir do Anexo I da Portaria SGD/MGI nº 1.070/2023.

Analista de suporte computacional (CBO 2124-20)	Profissional atuante em nível 3 em uma central de atendimento ou 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 e 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.
Administrador de banco de dados (CBO 2123-5)	Profissional responsável pela administração, operação, gerenciamento, otimização e monitoramento dos recursos de banco de dados. Presta serviços de gerenciamento dos esquemas de banco de dados, alocação e 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.
Administrador de sistemas operacionais (CBO 2123-15)	Profissional que atua na camada de virtualização e orquestração de sistema 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.
Analista de redes e de comunicação de dados (CBO 2124-10, 2123-10)	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.
Analista de sistemas de automação (CBO 2124-15, 2124-25)	Profissional responsável por assegurar a 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.
Desenvolvedor de sistemas de tecnologia da Informação (CBO 3171-10, 2124-30, 2124-05)	Profissional com a responsabilidade de assegurar a implantação adequada dos entregáveis de softwares. Pode atuar como analista de teste de aplicações executando testes automatizados e assegurando a cobertura mínima de testes nas soluções entregues. Pode atuar como analista de qualidade dos produtos a serem implantados.

Administrador em segurança da informação (CBO 2123-20)	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 de controle de segurança preventivo e reativo relacionados aos diferentes ativos da infraestrutura, bem como apoia na implementação das ações técnicas previstas na política de segurança.
---	--

2.

EQUIPES TÉCNICAS (SQUADS)

2.1.

Atividades Fundamentais Transversais

As seguintes atividades devem ser observadas por todas as categorias e perfis técnicos, alinhando-se aos processos de Gerenciamento de Serviços de TIC (GSTI) e às boas práticas (ITIL v4 e ISO/IEC 20000:2020).

ID	Descrição das Tarefas e Atividades
Geral-1	Realizar atividades de monitoramento preventivo (garantindo que serviços estejam livres de gargalos) e monitoramento proativo (averiguando falhas de segurança e esgotamento de infraestrutura).
Geral-2	Gerenciar e monitorar a performance e disponibilidade dos ativos, sistemas e serviços críticos.
Geral-3	Realizar configurações, alterações e otimizações no ambiente.
Geral-4	Tratar incidentes, problemas, requisições e mudanças.
Geral-5	Manter o ambiente atualizado observando as orientações previstas no Gerenciamento de Mudanças.
Geral-6	Acompanhar fornecedores e outros prestadores de serviços relacionados ao escopo do contrato, incluindo serviços de garantia e suporte técnico de terceiros.
Geral-7	Transformar continuamente as atividades humanas repetitivas de operação de infraestrutura de TIC por atividades automatizadas, como pelo uso de ferramentas de automação robótica de processos (RPA).
Geral-8	Elaborar e manter atualizada a documentação de todo o ambiente.
Geral-9	Identificar, mapear e atualizar o inventário de ativos de TIC (hardware e software).

2.2.

Atividades por Equipe Técnica

A seguir, apresento a organização das cinco categorias definidas no ETP, relacionando-as diretamente com as categorias da Portaria 1.070/2023 e suas alterações (incluindo a Portaria SGD/MGI nº 6.680/2024 e nº 6.055/2025).

2.2.1.

GOVERNANÇA DE SERVIÇOS DE TIC

a) **Escopo:** Governança técnica de serviços (incidente, mudança, problema, conhecimento), catálogo, NMS/indicadores; gestão de riscos e conformidade; reporte executivo. Esta categoria é o balizador central do modelo, sendo responsável por garantir a estabilidade e a

previsibilidade dos processos de Gerenciamento de Serviços de TI (GSTI), observando os padrões da ABNT NBR ISO/IEC 20000-1:2020.

b) Detalhamento não exaustivo de Tarefas e Atividades:

Gerenciamento de Serviços de TIC
Implantar e manter os processos de GSTI definidos pelo contratante, baseado nas melhores práticas.
Operar, manter, atualizar e criar fluxos de processos na ferramenta de Gerenciamento de Serviços de TIC (ITSM).
Adaptar os fluxos básicos de incidentes, requisição, mudanças, problemas e configuração, com o desenho de formulários e regras de validação.
Elaborar, manter e atualizar os relatórios de acompanhamento dos processos e indicadores de níveis de serviço (NMS).
Apoiar a STI na gestão do Catálogo de Serviços da DITEC, realizando a adição, supressão e modificação de itens.
Propor e implementar melhorias contínuas nos processos básicos de GSTI (ITIL).

c) Perfis Profissionais Necessários

PROFISSIONAL	PERFIL REFERÊNCIA (Portaria SGD/MGI nº 1.070/2023)	SENIORIDADE	Justificativa da senioridade
Analista de Serviços de TIC	Analista de suporte computacional	Junior	Apoio de qualidade/medição
Analista de Serviços de TIC	Analista de suporte computacional	Pleno	Pleno para operação GS/ITSM
Analista de Serviços de TIC	Analista de suporte computacional	Sênior	consolida padrões, automatiza rotinas e reduz reaberturas.

2.2.2. OPERAÇÃO DE DATACENTER

a) **Escopo:** Operação do NOC 24x7 (detecção/acionamento), plataformas de virtualização (VMware/Proxmox), storage/SAN, backup/restore e continuidade/DR, integrando monitoração técnica a SLO/Disponibilidade dos serviços finalísticos.

b) Detalhamento não exaustivo de Tarefas e Atividades:

Gerenciamento de Serviços de TIC
Implantar e manter os processos de GSTI definidos pelo contratante, baseado nas melhores práticas.
Operar, manter, atualizar e criar fluxos de processos na ferramenta de Gerenciamento de Serviços de TIC (ITSM).

Adaptar os fluxos básicos de incidentes, requisição, mudanças, problemas e configuração, com o desenho de formulários e regras de validação.
Elaborar, manter e atualizar os relatórios de acompanhamento dos processos e indicadores de níveis de serviço (NMS).
Apoiar a STI na gestão do Catálogo de Serviços da DITEC, realizando a adição, supressão e modificação de itens.
Propor e implementar melhorias contínuas nos processos básicos de GSTI (ITIL).

Armazenamento e Backup
Projetar, operar, administrar e manter o conjunto de soluções que compõem o ambiente de backup e armazenamento.
Executar, manter, atualizar, implantar e apoiar na criação das políticas de backup do contratante.
Realizar testes de restore com definição de frequência.
Administrar solução de backup (criação, edição e remoção de políticas, recuperação/restore).
Gerenciar a capacidade de storages, quotas e alocação de espaço.
Aplicar políticas de backup

Monitoramento de Serviços de TI
Realizar o monitoramento contínuo de sistemas de segurança física e subsistemas críticos do Centro de Certificação Digital (CCD/ITI), como climatização, CFTV, controle de acesso e alarmes (SIGAS).
Monitorar eventos de segurança, detectar intrusão e ameaças EDR em tempo real por meio da análise de logs (SIEM/EDR).
Relatórios mensais de disponibilidade e capacidade
Operação NOC (Zabbix/Prometheus/Grafana)

c) Perfis Profissionais Necessários

PROFISSIONAL	PERFIL REFERÊNCIA (Portaria SGD/MGI nº 1.070/2023)	SENIORIDADE	Justificativa da senioridade
Analista de Infraestrutura	Analista de suporte computacional	Pleno	Operar infraestrutura tecnológica do data center
Analista de Infraestrutura	Analista de suporte computacional	Sênior	Planejar a Gerenciar a operação do datacenter.

O Analista de Suporte Computacional (ASUPCOMP) é o profissional

associado ao centro de dados, responsável pelo gerenciamento físico e lógico de equipamentos, servidores, storages, e ambientes virtualizados. Suas atividades incluem o gerenciamento de backups e a configuração de procedimentos de recuperação de desastres computacionais.

Os ASUPCOMP são necessários no local para garantir a pronta resposta a incidentes e executar atividades físicas-operacionais de manutenção, como intervenção em servidores físicos e storages, sendo o acesso físico eventual limitado exclusivamente ao sítio localizado em Brasília/DF.

2.2.3. **SUSTENTAÇÃO DE APLICAÇÕES E BANCO DE DADOS**

- a) **Escopo:** Administração de sistemas de aplicação (Linux/Windows), automação de aplicações (CI/CD, IaC) e DBA (PostgreSQL/MySQL/SQL Server), com foco em alta disponibilidade e segurança.
- b) **Detalhamento não exaustivo de Tarefas e Atividades:**

Sustentação de Aplicações
Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõem a camada de sustentação de serviços e aplicações (servidores web/proxy, virtualização/containers, etc.).
Operar, administrar e manter os servidores físicos e virtuais.
Pipelines CI/CD e automação IaC
Realizar instalação, configuração e atualização de softwares básicos, SO e servidores de aplicação.
Gerenciar plataformas de virtualização/containers (orquestração e automação);
Administração de hosts/clusters e capacity/HA;
Execução de runbooks e readiness/execução de DR

Sustentação de Banco de Dados /Administração de Dados
Projetar, instalar, implantar, operar, administrar e manter o conjunto de ferramentas e softwares que compõem recursos e soluções relacionadas a bancos de dados.
Realizar configurações, alterações e otimizações no ambiente de banco de dados (ajuste de parâmetros, tuning).
Monitorar o desempenho, capacidade e continuidade dos SGBDs para detectar e corrigir eventuais problemas.
Sugerir e implantar sistemas de alta-disponibilidade (HA), cluster e replicação.
Utilizar ferramentas ETL de extração de dados, DW e Data Mining para o processamento de dados para fins de fiscalização e auditoria.
Construir mapas e processos de ETL (Extração, Transformação e Carga) e modelar dados para apoiar a equipe de desenvolvimento de sistemas.
DBA (tuning/replicação/HA/restore de prova)

Monitoramento de Serviços de TI

Hardening/tuning e monitoração de aplicação
Relatórios técnicos (mudanças, desempenho, disponibilidade)
Fornecer informações táticas e operacionais e relatórios sobre o desempenho dos serviços de infraestrutura que suportam a DITEC e DAFN.

c) Perfis Profissionais Necessários

PROFISSIONAL	PERFIL REFERÊNCIA (Artaria SGD/MGI nº 1.070/2023)	SENIORIDADE	Justificativa da senioridade
Administrador de Plataformas	Administrador de sistemas operacionais	Pleno	Atividades com grau de complexidade, requerendo capacidade de análise crítica e resolução de problemas. Estes profissionais formam o núcleo de execução, realizando configurações, alterações, otimizações e manutenção preventiva e corretiva nos servidores físicos e virtuais.
Administrador de Plataformas	Administrador de sistemas operacionais	Sênior	São necessários para exercer atividades com grau elevado de complexidade e criticidade. Este nível é fundamental para projetar, implementar e manter os sistemas operacionais e ambientes de <i>containers</i> em um contexto de segurança reforçada e conformidade normativa, liderando as ações de Sustentação de Infraestrutura para Aplicações e resolvendo incidentes complexos.

Analista DevOps	Analista de Sistemas de Automação	Pleno	É o perfil adequado para exercer atividades com grau de complexidade, que requerem maior capacidade de análise crítica e resolução de problemas. Tais competências são vitais para a implementação, manutenção e aprimoramento das arquiteturas de automação e DevSecOps em um ambiente de segurança extrema.
Analista de Banco de Dados	Administrador de banco de dados	Pleno	Exercer atividades com grau elevado de complexidade e criticidade, exigindo experiência e qualificação profissional, Monitorar incidentes e realizar pronto atendimento em ambiente 24x7. Realizar Tuning de Banco de Dados, otimizar consultas e performance, e propor padrões e a normalização de dados corporativos.
Administrador de Banco de Dados	Administrador de banco de dados	Sênior	Exercer atividades com grau elevado de complexidade e criticidade, exigindo experiência e qualificação profissional diferenciada. Implantar soluções de Alta Disponibilidade e gerenciar ambientes de missão crítica.

O ITI, na qualidade de AC Raiz da ICP-Brasil e responsável pela infraestrutura das Assinaturas Eletrônicas Avançadas do portal Gov.BR e da Carteira de Identidade Nacional (CIN), exige operação contínua, segura e auditável (24x7x365) e alta disponibilidade de 99,99%.

O Analista de Sistemas de Automação (ASISA) é o profissional crucial para garantir a eficiência e a segurança, sendo responsável por:

- Assegurar a utilização adequada de soluções de Integração Contínua (CI) ou Entrega Contínua (CD).
- Atuar como arquiteto de soluções, propondo, projetando e aprimorando arquiteturas.

- Promover a transformação de atividades humanas repetitivas de manutenção por atividades automatizadas (e.g., RPA - *Robotic Process Automation*).

O Administrador de Sistemas Operacionais (ASO) é essencial para esta sustentação, pois atua na camada de virtualização e orquestração de sistemas operacionais de servidores de dados, sendo responsável pela adequada operação, desempenho e uso racional de recursos utilizados por *softwares* básicos, orquestradores de *containers* (Ex. Kubernetes) e virtualizadores.

O ambiente tecnológico do ITI, que utiliza arquitetura de tríplice clusterização e possui servidores com sistemas operacionais descontinuados que precisam de atualização, demanda alta especialização:

O serviço de Sustentação de Banco de Dados (SustSGBD) é essencial e exige profissionais que:

- Projetem, instalem, implantem, operem, administrem e mantenham o conjunto de *softwares* e *hardwares* de bancos de dados.
- Gerenciem esquemas de banco de dados, alocação de recursos físicos e lógicos, realizem dimensionamentos, monitorem incidentes e promovam expansão dos recursos.
- Realizem configurações, alterações e otimizações no ambiente de banco de dados.
- A sustentação de banco de dados é uma das categorias de serviço de TIC que suporta estas iniciativas estratégicas.

2.2.4. INFRAESTRUTURA DE REDES E CONECTIVIDADE

a) **Escopo:** Operação e evolução de LAN/WAN/VPN, segmentação (VLAN), QoS e integração com NOC/SOC, garantindo conectividade estável aos serviços finalísticos.

b) **Detalhamento não exaustivo de Tarefas e Atividades:**

Conectividade e Comunicação
Projetar, operar, administrar e manter o conjunto de soluções, ferramentas e hardwares que compõem o ambiente de conectividade e comunicação (redes, switches, roteadores, links, VPNs);
Realizar configurações, alterações e otimizações no ambiente de conectividade e comunicação;
Gerenciar enlaces de longa distância (WAN/MPLS) e serviços de VPN site-to-site;
Provisionamento/configuração de switches/roteadores;
Gestão de VLANs, VPNs e QoS;
Troubleshooting de L2/L3;
Documentação topológica;
Integração com NOC/SOC;
Higiene de regras.

c) Perfis Profissionais Necessários

PROFISSIONAL	PERFIL REFERÊNCIA (Portaria SGD/MGI nº 1.070/2023)	SENIORIDADE	Justificativa da senioridade
Analista NOC N2	Analista de redes e de comunicação de dados	Pleno	Exige capacidade de análise crítica e resolução de problemas. A exigência de ser presencial é crucial para tarefas que demandam acesso físico ao Centro de Certificação Digital (CCD/ITI), como a instalação, substituição ou remoção de equipamentos, roteadores e <i>switches</i> , bem como a organização de cabeamento e o acompanhamento de fornecedores.
Analista NOC N3	Analista de redes e de comunicação de dados	Sênior	Adequados para exercer atividades com grau elevado de complexidade e criticidade, requerendo experiência e qualificação profissional diferenciada. Devem focar em tarefas de alta complexidade, como projeto, otimização de arquitetura de redes (IPv4/IPv6, VPN site to site, roteamento) e resolução de incidentes de rede.

A contratação de Analistas de Redes e de Comunicação de Dados (ARED) é condição indispensável para a continuidade institucional do ITI. O dimensionamento misto de senioridade e regime de atuação é fundamental para garantir a operação contínua, segura e auditável da infraestrutura de TIC que suporta a Autoridade Certificadora Raiz (AC Raiz) da ICP-Brasil, as Assinaturas Eletrônicas Avançadas do portal Gov.BR e a Carteira de Identidade Nacional (CIN), que demandam operação ininterrupta e alta disponibilidade (99,99%).

O Analista de redes e de comunicação de dados é o profissional responsável por projetar, operar, administrar e manter o ambiente de conectividade e comunicação do contratante. Isso inclui a gestão de redes locais e de longa distância (LAN / MAN / WAN), a configuração e otimização de ativos de redes, e o tratamento de incidentes e problemas relacionados à comunicação.

A divisão entre o regime remoto para a expertise sênior estratégica e o regime presencial para as operações físicas e suporte *on-site* nos ambientes seguros é essencial para a gestão da infraestrutura de redes (Conectividade e Comunicação) e para assegurar a resiliência e a disponibilidade contínua dos serviços críticos do ITI. A contratação adere ao modelo da Portaria SGD/MGI nº 1.070/2023, sendo remunerada por resultados (NMS).

2.2.5. CIBERSEGURANÇA

a) **Escopo:** Dada a natureza da ICP-Brasil, a Cibersegurança exige atenção especial à conformidade (DOC-ICP, LGPD). Operação do SOC 24x7 (detecção/triagem/resposta), perímetro (NGFW/WAF/IPS), Contas de Usuários, tratamento de vulnerabilidades e hardening, com ênfase em requisitos ICP-Brasil e LGPD. Incluem a implantação e operação do SOC (Security Operations Center) para monitoramento contínuo (24x7x365), a proteção de perímetro (Firewalls, IPS/IDS, WAF), realização de testes de vulnerabilidades, e o apoio na elaboração de políticas de segurança, planos de continuidade de negócio e gestão de riscos.

b) **Detalhamento não exaustivo de Tarefas e Atividades:**

Segurança de TIC
Implantar e operar o SOC (Security Operations Center) para monitoramento contínuo (24x7x365) de segurança;
Projetar, operar, administrar e manter o conjunto de soluções, ferramentas e hardwares que compõem o ambiente de segurança de TIC (firewall, IPS/IDS, WAF, antivírus);
Realizar testes de vulnerabilidades dos sistemas e serviços de TIC (Pentest) e sugerir ações de tratamento;
Tratar incidentes, problemas e requisições relacionados à segurança de TIC;
Gerenciamento de Credenciais e Acessos : Criação, modificação, inativação e exclusão de perfis e atributos de contas e senhas para acesso lógico aos sistemas da AC Raiz;
Apoiar na elaboração e manutenção da política de segurança, plano de continuidade de negócio e plano de gerenciamento de risco;
Garantir que o ambiente de produção e não produção estejam segregados;
Monitoração SIEM/EDR;
Gestão de regras NGFW/WAF/IPS;
Varredura e patch;
Forense básica;
Relatórios de conformidade.

c) **Perfis Profissionais Necessários**

PROFISSÃO	PERFIL REFERÊNCIA (Arbitaria SGD/MGI nº 1.070/2023)	SENIORIDADE	Justificativa da senioridade
-----------	---	-------------	---------------------------------

Analista SOC N1	Administrador em segurança da informação	Junior	São adequados para tarefas de menor complexidade, prestando suporte na implementação das ações técnicas previstas na política de segurança e em controles de segurança preventivos e reativos.
Analista SOC N2	Administrador em segurança da informação	Pleno	São necessários para atividades de maior grau de complexidade, exigindo maior análise crítica e resolução de problemas. Estes profissionais são o núcleo operacional responsável pelo Gerenciamento de Segurança de Perímetro (firewall, IPS/IDS) e pela operação do SOC (Security Operations Center), garantindo o monitoramento contínuo (24x7x365).
Analista SOC N3	Administrador em segurança da informação	Sênior	É essencial para atividades com grau elevado de complexidade e criticidade, como a definição de arquitetura de segurança, liderança em resposta rápida a ataques e incidentes, apoio na elaboração da política de segurança e realização de Pentest.

O ITI não possui quadro próprio de pessoal suficiente para sustentar essa complexidade, sendo a contratação externa a única solução viável para o serviço de Segurança de TIC, que inclui projetar, operar, administrar, manter soluções, tratar incidentes de segurança e realizar testes de vulnerabilidades e Penetration Test (Pentest).

O escalonamento dos perfis é determinado pela natureza, criticidade e complexidade dos serviços a serem prestados. A área de segurança da informação (ASEG) é altamente sensível e exige aderência rigorosa a normativos como a Política de Segurança da ICP-Brasil (DOC-ICP-02) e a POSIN/ITI.

Portanto, a composição visa equilibrar a necessidade de expertise sênior para planejamento e gestão de ameaças, com a presença Pleno e Júnior para a

sustentação, monitoramento e resposta imediata dentro do Ambiente Seguro do ITI.

2.2.6. **GOVERNANÇA DE SERVIÇOS NEGOCIAIS DITEC**

Esta Equipe, considerando sustentação de infra de TIC" refere-se à contratação de serviços técnicos especializados de Tecnologia da Informação e Comunicação (TIC), em regime de execução indireta, para a Diretoria de Infraestrutura Tecnológica (DITEC). Sugere que o foco está no planejamento, gestão da qualidade, segurança preventiva, e sustentação técnica complexa, essenciais para a evolução proativa do ambiente crítico.

Foco de Atuação	Justificativa de Alinhamento à DITEC
Qualidade, Conformidade e Sustentação de Aplicações.	Responsável por garantir a implantação contínua e integrada dos entregáveis de software, atuando na validação de qualidade, testes automatizados e monitoramento de aplicações, com foco na confiabilidade, desempenho e melhoria contínua dos produtos.
Segurança e Gerenciamento de Riscos	Responsável por assegurar a prestação de serviços de segurança da informação, tratando incidentes e realizando configurações e otimizações no ambiente de segurança de TIC.

Em resumo, a equipe é um *pool* de especialistas focado em modernizar, automatizar, garantir a qualidade e manter a segurança e a conformidade técnica visando a resiliência dos Serviços Negociais da DITEC.

a) **Escopo:** Squad técnico próximo ao negócio para sustentar AC Raiz, Assinaturas Avançadas, EAT, TLSO, focado em automação de aplicações (ASISA/DESTEC), SLO de serviço e segurança aplicada com trilhas de auditoria. Esta é uma categoria customizada que combina funções de gestão (Governança) e execução técnica especializada (Sustentação Nível 3), focada nos serviços finalísticos da DITEC (AC Raiz, Assinaturas Avançadas).

b) **Detalhamento não exaustivo de Tarefas e Atividades:**

Sustentação de Aplicações
Projetar, operar, administrar e manter o conjunto de soluções, ferramentas, softwares e hardwares que compõem a camada de sustentação de serviços e aplicações (servidores web/proxy, virtualização/containers, etc.).
Operar, administrar e manter os servidores físicos e virtuais.
Realizar instalação, configuração e atualização de softwares básicos, SO e servidores de aplicação em ambiente de desenvolvimento, teste e homologação
Automação de fluxos e esteiras do serviço

Monitoramento de Serviços de TI
Fornecer informações táticas e operacionais e relatórios sobre o desempenho dos serviços de infraestrutura que suportam a DITEC.
Testes sintéticos e observabilidade orientada a serviço
Readiness e pós-implantação de mudanças

c) **Perfis Profissionais Necessários:** O perfil da equipe alocada nesta categoria (Analista de Suporte Computacional - Pleno, Desenvolvedor de Sistemas de TI, Analista de Sistemas de Automação, Administrador em Segurança da Informação) demonstra que o trabalho foca em **Sustentação de Aplicações, Segurança de TIC e Monitoramento de Serviços de TI** (através da automação e engenharia de infraestrutura - DevSecOps). As atividades visam modernizar, automatizar e garantir a qualidade da infraestrutura.

PROFISSIONAL	PERFIL REFERÊNCIA (Portaria SGD/MGI nº 1.070/2023)	SENIORIDADE	Justificativa da senioridade
Analista de Integração e Testes de Software	Desenvolvedor de sistemas de tecnologia da informação	Pleno	Necessário para exercer atividades de maior grau de complexidade, que exigem maior capacidade de análise crítica e resolução de problemas, atuando em sistemas que suportam a tríple clusterização e a criticidade da AC Raiz
Especialista em Segurança e Operações de Serviços	Administrador em segurança da informação	Pleno	Devido à missão crítica e à exigência de conformidade contínua

A contratação de "Desenvolvedor de Sistemas de TI Pleno é uma condição indispensável para a continuidade institucional do ITI, visando a Sustentação de Aplicações.

Esta necessidade se justifica pela:

- Missão Crítica e Operação Ininterrupta: O ITI é a AC Raiz da ICP-Brasil e responsável por plataformas de altíssima criticidade, como as Assinaturas Eletrônicas Avançadas do portal Gov.BR. Estes ambientes exigem operação contínua, segura e auditável e alta disponibilidade (99,99%).
- Função de Sustentação: O Desenvolvedores de Sistema de TI (DESTEC) é responsável por garantir a implantação adequada dos

entregáveis de softwares. Suas atividades incluem validação de scripts e pipelines de automação para provisionamento de infraestrutura, execução de testes automatizados e manuais, monitoramento de indicadores de qualidade, e garantia de conformidade com padrões técnicos e requisitos de segurança. O ITI adota modelos baseados em DevOps/DevSecOps, o que exige competências em Controle de versão, Integração contínua e Deployment.

- Em suma, a contratação é essencial para suprir a ausência de quadro próprio e garantir que a infraestrutura de desenvolvimento e sustentação dos serviços críticos do ITI se mantenha operacional e segura em regime ininterrupto.

2.2.7. GOVERNANÇA DE SERVIÇOS NEGOCIAIS DAFN

A DAFN é a diretoria responsável por fiscalizar e normalizar (estabelecer regras técnicas) a ICP-Brasil. O seu papel é de asseguração e controle de conformidade. Esta Equipe Técnica, com foco em sustentação de infraestrutura de Tecnologia da Informação e Comunicação (TIC), descreve a contratação de serviços técnicos especializados para apoiar e aprimorar a gestão da infraestrutura de TIC que suporta as atividades finalísticas da DAFN: Auditoria, Fiscalização e Normalização. De forma que os serviços são classificados como uma Solução de TIC, especificamente para a Operação de Infraestrutura de TIC, que inclui a prestação de serviços técnicos relacionados à segurança da informação, banco de dados, servidores, monitoramento e gerenciamento operacional.

Foco de Atuação	Justificativa de Alinhamento à DAFN
Qualidade e Automação	Estes profissionais focam em Melhoria Contínua e Automação de Processos, sendo responsáveis por assegurar a utilização adequada de soluções de CI/CD. Essa competência é vital para a DAFN garantir que os sistemas estruturantes de auditoria e normalização sejam evoluídos com qualidade e conformidade, minimizando intervenções manuais.
Gestão e Segurança de Dados Críticos	O Administrador de Banco de Dados Sênior apoia as atividades de Administração de Dados (categoria da Portaria 1070), incluindo auditoria, análise de documentação de modelagem e manutenção de esquemas de banco de dados. O foco em segurança (Administradores de SI) visa a segurança preventiva e reativa do ambiente que suporta as funções de fiscalização e normatização.
Sustentação de Aplicações e Testes	Estes perfis asseguram a implantação adequada dos entregáveis de <i>softwares</i> e atuam como analistas de teste de aplicações, fundamentais para garantir a qualidade (Desenho e Transição de Serviço) de quaisquer ferramentas ou sistemas que a DAFN utilize ou adquira (como as licenças de <i>software</i> de auditoria e banco de dados mencionadas no PDTIC).

Em síntese, consiste na provisão de um time de especialistas, remunerado por resultados (NMS), dedicado a garantir a qualidade técnica, a

conformidade normativa, a segurança e a automação do ambiente de TIC necessário para suportar as complexas funções de auditoria, fiscalização e normalização do órgão.

Cada uma das categorias de serviços será responsável por atuar em um determinado segmento da cadeia de prestação de serviços, de acordo com a sua especialidade, de modo a garantir a observância dos níveis de serviço e desempenho estabelecidos.

a) Escopo: Equipe técnica lado a lado com as áreas DAFN para sustentar serviços de negócio, com automação, monitoramento por jornada e segurança aplicada (dados pessoais e legais). Categoria customizada para apoiar as atividades finalísticas da DAFN (Auditoria, Fiscalização e Normalização), sendo classificada como uma Solução de TIC de Operação de Infraestrutura. Apoio especializado à Diretoria de Auditoria, Fiscalização e Normalização (DAFN) em termos de qualidade, conformidade normativa, ETL e segurança da informação para bases de auditoria.

b) Detalhamento não exaustivo de Tarefas e Atividades:

Sustentação de Aplicações / Sustentação de Banco de Dados
Atuar como analista de teste de aplicações e garantir a qualidade (Desenho e Transição de Serviço) de quaisquer ferramentas ou sistemas que a DAFN utilize ou adquira.
Administrar, Operar e Suportar Banco de Dados para sistemas de fiscalização e bases de auditoria.
Automação de integrações e ajustes de esteiras do serviço
Segurança de TIC
Apoiar a auditoria de segurança e a manutenção da conformidade com a LGPD.
Apoiar na identificação, mapeamento e análise dos riscos e na elaboração de planos de ação apropriados para os riscos identificados (DITEC e DAFN).
Administração de Dados
Utilizar ferramentas ETL de extração de dados, DW e Data Mining para o processamento de dados para fins de fiscalização e auditoria.
Construir mapas e processos de ETL (Extração, Transformação e Carga) e modelar dados para apoiar a equipe de desenvolvimento de sistemas da DAFN.
Monitoramento de Serviços de TI
Fornecer informações táticas e operacionais e relatórios sobre o desempenho dos serviços de infraestrutura que suportam a DAFN.
Probes de teste e observabilidade orientada à experiência do usuário
Evidências de conformidade e interface contínua com a área de negócio

c) Perfis Profissionais Necessários: O perfil (Analistas de Sistemas de Automação, Desenvolvedor de Sistemas de TI) é direcionado para a Qualidade, Automação, Sustentação de Aplicações e Testes. Essas atividades são essenciais para garantir que os sistemas estruturantes de auditoria e normalização sejam evoluídos com qualidade e conformidade, utilizando competências que se enquadram nas categorias de Sustentação de Aplicações, Administração de Dados e Segurança de TIC da Portaria 1.070/2023.

PROFISSIONAL	PERFIL REFERÊNCIA (Portaria SGD/MGI nº 1.070/2023)	SENIORIDADE	Justificativa da senioridade
Analista de Sistemas de Automação	Analista de Sistemas de Automação	Pleno	É o perfil adequado para exercer atividades com maior grau de complexidade, que requerem maior capacidade de análise crítica e resolução de problemas. Tais competências são vitais para a implementação, manutenção e aprimoramento das arquiteturas de automação e DevSecOps em um ambiente de segurança extrema.
Administrador de Dados	Administrador de banco de dados	Sênior	Integrações/controles sensíveis
Analista de Segurança de Dados	Administrador em segurança da informação	Junior	Apoio operacional acerca da segurança em especial análises antifraude
Analista de Auditoria e Conformidade	Administrador em segurança da informação	Pleno	Automação/observabilidade

3. PROPOSTA DE USO DE AUTOMAÇÃO POR EQUIPE TÉCNICA

- I. **GOVERNANÇA DE SERVIÇOS DE TIC:** Workflows ITSM, SLAs/NMS automáticos e integrações com NOC/SOC, Imaging/templates e distribuição de software; Chatbots e base de conhecimento integrados ao ITSM
- II. **OPERAÇÃO DE DATACENTER:** IaC/Ansible para padronização de builds e configurações; Dashboards de disponibilidade e relatórios automáticos ao ITSM
- III. **SUSTENTAÇÃO DE APLICAÇÕES E BANCO DE DADOS:** CI/CD (GitLab/Jenkins/ArgoCD) e IaC (Ansible/Terraform); Testes automatizados, canary/blue-green, scripts de verificação
- IV. **INFRAESTRUTURA DE REDES E CONECTIVIDADE:** Templates/scripts de

configuração e captura de telemetria; Integração de traps/telemetria com NOC

- V. **CIBERSEGURANÇA:** Playbooks de resposta (SOAR) e varredura automatizada; Políticas como código e validações contínuas
- VI. **GOVERNANÇA DE SERVIÇOS NEGOCIAIS DITEC:** CI/CD e IaC por serviço; SLO dashboards; segurança como código
- VII. **GOVERNANÇA DE SERVIÇOS NEGOCIAIS DAFN:** CI/CD e IaC por serviço; dashboards SLO; listas de verificação de conformidade



Documento assinado eletronicamente por **Rafael de Lima Ramos, Coordenador(a)**, em 01/09/2026, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Alysson Marques, Coordenador-Geral**, em 01/09/2026, às 11:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0810874** e o código CRC **A39E8C93**.

Referência: Processo nº 00100.002198/2025-02

SEI nº 0810874

LICITAÇÃO: ANEXO Nº ETP 6/2026 - APÊNDICE IV -/2026/ASSESSOR-DITEC/DITEC

Processo nº 00100.002198/2025-02

Interessado: CGISE

APÊNDICE IV - QUALIFICAÇÃO DOS PROFISSIONAIS

1. DISPOSIÇÕES GERAIS

Em razão da criticidade do ambiente do CONTRATANTE, serão exigidos profissionais com as qualificações técnicas mínimas descritas neste documento.

A CONTRATADA terá no máximo 3 (três) meses, após a emissão da primeira Ordem de Serviço (OS), para adequação de todas as certificações dos perfis profissionais requeridos. Após esse período, o profissional sem as certificações da referida Categoria de Serviços não estará mais apto a atuar na resolução dos chamados e a CONTRATADA receberá glosas contratuais por não preencher os critérios e o perfil profissional requisitado na OS.

Os profissionais da CONTRATADA que apresentarão as certificações exigidas são os que atuarão e terão credenciais de acesso na infraestrutura de TIC da DITEC/ITI, não podendo a CONTRATADA apresentar certificações para os perfis e designar outros profissionais para a execução do objeto.

A critério da DITEC/ITI, poderão ser aceitas comprovações alternativas de graduação, certificações, conhecimentos e experiências em substituição às indicadas neste documento, desde que apresentadas pela CONTRATADA de forma fundamentada e justificada.

Diplomas e certificados utilizados para comprovação da formação acadêmica devem ser devidamente registrados e fornecidos por instituição de ensino reconhecida pelo MEC.

Para comprovação do tempo mínimo de experiência, admite-se a soma de diversas experiências, desde que não simultâneas.

Participação em treinamentos deverá ser comprovada por meio de certificado de conclusão ou certificado de proficiência obtido em prova oficial do fabricante cujo treinamento requisitado seja parte da preparação.

Caso alguma certificação seja descontinuada durante a vigência contratual, passará a ser exigida a certificação que a substituir para a validação da qualificação de novos profissionais.

O quadro a seguir apresenta a relação dos perfis profissionais, organizados por Equipe Técnica (squad), com seus respectivos perfis de referência, códigos de identificação, CBOs de referência e função:

EQUIPE TÉCNICA	CATEGORIA DE SERVIÇOS (Portaria SGD/MGI nº 1.070/2023)	PROFISSIONAL	PERFIL REFERÊNCIA (Portaria SGD/MGI nº 1.070/2023)	CBO (Portaria SGD/MGI nº 1.070/2023)	COD PERFIL REFERÊNCIA (Portaria SGD/MGI nº 1.070/2023)	SENIORIDADE
GOVERNANÇA DE SERVIÇOS DE TIC	Monitoramento de Serviços de TI / Gerenciamento de Serviços de TIC	Analista de Serviços de TIC	Analista de suporte computacional	2124-20	ASUPCOMP-01	Junior
	Monitoramento de Serviços de TI / Gerenciamento de Serviços de TIC	Analista de Serviços de TIC	Analista de suporte computacional	2124-20	ASUPCOMP-02	Pleno
	Monitoramento de Serviços de TI / Gerenciamento de Serviços de TIC	Analista de Serviços de TIC	Analista de suporte computacional	2124-20	ASUPCOMP-03	Sênior
OPERAÇÃO DE DATACENTER	Monitoramento de Serviços de TI / Armazenamento e Backup	Analista de Infraestrutura	Analista de suporte computacional	2124-20	ASUPCOMP-02	Pleno
	Monitoramento de Serviços de TI / Armazenamento e Backup	Analista de Infraestrutura	Analista de suporte computacional	2124-20	ASUPCOMP-03	Sênior
SUSTENTAÇÃO DE APLICAÇÕES E BANCO DE DADOS	Sustentação de Aplicações	Administrador Plataformas	Administrador de sistemas operacionais	2123-15	ASO-02	Pleno
	Sustentação de Aplicações	Administrador Plataformas	Administrador de sistemas operacionais	2123-15	ASO-03	Sênior
	Sustentação de Aplicações	Analista DevOps	Analista de Sistemas de Automação	2124-15, 2124-25	ASISA-02	Pleno
	Sustentação de Banco de Dados	Analista de Banco de Dados	Administrador de banco de dados	2123-5	ABD-02	Pleno
	Administração de Dados	Administrador de Banco de Dados	Administrador de banco de dados	2123-5	ABD-03	Sênior

INFRAESTRUTURA DE REDES E CONECTIVIDADE	Conectividade e Comunicação	Analista NOC N2	Analista de redes e de comunicação de dados	2124-10, 2123-10	ARED-02	Pleno
	Conectividade e Comunicação	Analista NOC N3	Analista de redes e de comunicação de dados	2124-10, 2123-10	ARED-03	Sênior
CIBERSEGURANÇA	Segurança de TIC	Analista SOC N1	Administrador em segurança da informação	2123-20	ASEG-01	Junior
	Segurança de TIC	Analista SOC N2	Administrador em segurança da informação	2123-20	ASEG-02	Pleno
	Segurança de TIC	Analista SOC N3	Administrador em segurança da informação	2123-20	ASEG-03	Sênior
GERENCIAMENTO E EXECUÇÃO DE SERVIÇOS NEGOCIAIS DITEC	Sustentação de Aplicações	Analista de Integração e Testes de Software	Desenvolvedor de sistemas de tecnologia da informação	3171-10, 2124-30, 2124-05	DESTEC-02	Pleno
	Monitoramento de Serviços de TI	Analista em Segurança e Operações de Serviços	Administrador em segurança da informação	2123-20	ASEG-02	Pleno
GERENCIAMENTO E EXECUÇÃO DE SERVIÇOS NEGOCIAIS	Sustentação de Aplicações	Analista de Sistemas de Automação	Analista de Sistemas de Automação	2124-15, 2124-25	ASISA-02	Pleno
	Sustentação de Banco de Dados / Administração de Dados	Administrador de Dados	Administrador de banco de dados	2123-5	ABD-03	Sênior
	Monitoramento de Serviços de TI	Analista de Segurança de Dados	Administrador em segurança da informação	2123-20	ASEG-01	Junior

DAFN						
	Monitoramento de Serviços de TI	Analista de Auditoria e Conformidade	Administrador em segurança da informação	2123-20	ASEG-02	Pleno

* Portaria SGD/MGI nº 1.070/2023

2. QUALIFICAÇÕES DOS PROFISSIONAIS

2.1. Requisitos Gerais de experiência, formação e certificações

I - Tempo de Experiência

Modo de comprovação: 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) Perfil Júnior: Um (01) ano;
- b) Perfil Pleno: Três (03) anos;
- c) Perfil Sênior: Cinco (05) anos.

II - Formação

a) Para o perfil "**Técnico em manutenção de equipamentos de informática**", o colaborador deve possuir ensino médio completo ou curso técnico equivalente, em curso reconhecido pelo Ministério da Educação. **Modo de Comprovação:** Diploma, devidamente registrado, de conclusão de curso, fornecido por instituição de ensino reconhecida pelo Ministério da Educação – MEC.

b) **Para os demais perfis:** Possuir diploma de conclusão de curso de nível superior na área de Tecnologia da Informação, em curso reconhecido pelo Ministério da Educação ou nível superior completo em outra área, com pós-graduação, mestrado ou doutorado na área de Tecnologia da Informação, em curso reconhecido pelo MEC. **Modo de Comprovação:** Diploma, devidamente registrado, de conclusão de curso, fornecido por instituição de ensino superior reconhecida pelo Ministério da Educação – MEC.

III - Cursos e/ou Certificações obrigatórias

Possuir certificação ou curso no exame de:

- a) ITIL v3 ou superior, com carga horária mínima de vinte (20) horas;
- b) Gestão de Segurança da Informação (SGSI)/ ABNT NBR ISO/IEC

27001:2022, com carga horária mínima de vinte (20) horas.

c) Modo de Comprovação: Certificados emitidos por instituição formadora.

2.2. Por Equipe Técnica (squad)

I - GOVERNANÇA DE SERVIÇOS DE TIC

Perfil Profissional	Certificações Obrigatórias	Experiência Profissional
Analista de Serviços de TIC Júnior	Deve possuir curso de Sistema de Gerenciamento de Serviços de TIC, ABNT NBR ISO/IEC 20000-1:2020, com carga horária mínima de 20 horas. Deve possuir curso de requisitos para sistemas de gestão da qualidade / ABNT NBR ISO 9001:2015, com carga horária mínima de 20 horas.	Experiência mínima pelo tempo definido para o nível de senioridade na área de serviços de TIC.
Analista de Serviços de TIC Pleno	Deve possuir curso de Sistema de Gerenciamento de Serviços de TIC, ABNT NBR ISO/IEC 20000-1:2020, com carga horária mínima de 20 horas. Deve possuir curso de requisitos para sistemas de gestão da qualidade / ABNT NBR ISO 9001:2015, com carga horária mínima de 20 horas.	Experiência mínima pelo tempo definido para o nível de senioridade na área de serviços de TIC.
Analista de Serviços de TIC Sênior	Deve possuir curso de Sistema de Gerenciamento de Serviços de TIC, ABNT NBR ISO/IEC 20000-1:2020, com carga horária mínima de 20 horas. Deve possuir curso de requisitos para sistemas de gestão da qualidade / ABNT NBR ISO 9001:2015, com carga horária mínima de 20 horas.	Experiência mínima pelo tempo definido para o nível de senioridade na área de serviços de TIC.

II - OPERAÇÃO DE DATACENTER

Perfil Profissional	Certificações Obrigatórias	Experiência Profissional
Analista de Infraestrutura Pleno		Experiência mínima pelo tempo definido para o nível de senioridade

		em atividades de instalação, manutenção e configuração de hardware, incluindo servidores do tipo rack, configuração da gerência remota de equipamentos. Além de experiência em gerenciamento e monitoração de ambiente de datacenter.
Analista de Infraestrutura Sênior		

III - SUSTENTAÇÃO DE APLICAÇÕES E BANCO DE DADOS

Perfil Profissional	Certificações Obrigatórias	Experiência Profissional
Administrador Plataformas Pleno	No mínimo um integrante da área deve possuir Certificação Linux LPI-I;	Experiência mínima pelo tempo definido para o nível de senioridade em administração de sistemas de virtualização VMWare ou similares, e com gerência e orquestração de ambiente virtualizado
Administrador Plataformas Sênior		
Analista DevOps Pleno	No mínimo uma das seguintes certificações: Certificação Certified Kubernetes Administrator (CKA) ou superior; Certificação Certified Kubernetes Application Developer (CKAD).	Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.
Analista de Banco de Dados Pleno	No mínimo um integrante deve possuir certificação: Certificação SQL Server 2016 ou equivalente; MySQL for Database Administrators ou superior.	Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.
Administrador de Banco de Dados Pleno		Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.

IV - INFRAESTRUTURA DE REDES E CONECTIVIDADE

Perfil Profissional	Certificações Obrigatórias	Experiência Profissional
Analista NOC N2 Pleno	No mínimo um integrante da área deve possuir uma	Experiência mínima pelo tempo

	das seguintes certificações:	definido para o nível de senioridade na administração de
Analista NOC N3 Sênior	1. Certificação Cisco Certified Network Associate (CCNA) ou equivalente; 2. Certificação CCNP Security – Cisco Certified Network Professional Security.	ambiente de Rede TCP/IP e MPLS, roteadores, gateway de voz, switches, VLAN, segurança de redes, endereçamento e roteamento IP, GPON, protocolos autônomos de roteamento (BGP, OSPF), implantação de QoS em redes corporativas.

V - CIBERSEGURANÇA

Perfil Profissional	Certificações Obrigatórias	Experiência Profissional
Analista SOC N1 Junior		Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.
Analista SOC N2 Pleno	No mínimo um integrante da área deve possuir Certificação Auditor Líder ISO/IEC 27001 ou CISSP.	Experiência mínima pelo tempo definido para o nível de senioridade na área de redes ou segurança da Informação.
Analista SOC N3 Sênior		Experiência mínima pelo tempo definido para o nível de senioridade na área de Segurança da Informação, acrescido de Pós-graduação na área de Segurança da Informação.

VI - GOVERNANÇA DE SERVIÇOS NEGOCIAIS DITEC

Perfil Profissional	Certificações Obrigatórias	Experiência Profissional
Analista de Integração e Testes de Software Pleno	No mínimo uma das seguintes certificações: Certificação Certified Kubernetes Administrator (CKA) ou superior; Certificação Certified Kubernetes Application Developer (CKAD).	Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.

Analista em Segurança e Operações de Serviços Pleno		Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.

VII - GOVERNANÇA DE SERVIÇOS NEGOCIAIS DAFN

Perfil Profissional	Certificações Obrigatórias	Experiência Profissional
Analista de Sistemas de Automação Pleno	No mínimo uma das seguintes certificações: Certificação Certified Kubernetes Administrator (CKA) ou superior; Certificação Certified Kubernetes Application Developer (CKAD).	Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.
Administrador de Dados Sênior	No mínimo um integrante deve possuir certificação: Certificação SQL Server 2016 ou equivalente; MySQL for Database Administrators ou superior.	Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.
Analista de Segurança de Dados Junior		Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.
Analista de Auditoria e Conformidade Pleno		Experiência mínima pelo tempo definido para o nível de senioridade em tecnologia da informação.



Documento assinado eletronicamente por **Rafael de Lima Ramos, Coordenador(a)**, em 01/09/2026, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Alysson Marques, Coordenador-Geral**, em 01/09/2026, às 11:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0810876** e o código CRC **753F4DB9**.

Referência: Processo nº 00100.002198/2025-02

SEI nº 0810876

LICITAÇÃO: ANEXO Nº ETP 6/2026 - APÊNDICE V -/2026/ASSESSOR-DITEC/DITEC

Processo nº 00100.002198/2025-02

Interessado: CGISE

APÊNDICE V - INDICADORES DE NÍVEIS DE SERVIÇOS

1. DISPOSIÇÕES GERAIS

- 1.1. Os serviços contratados terão sua qualidade aferida por meio de critérios objetivos e mensuráveis. Para mensurar esses fatores serão utilizados indicadores relacionados com a natureza e característica dos serviços contratados.
- 1.2. A CONTRATADA deverá atender os níveis de serviço e desempenho aqui detalhados, atentando-se também aos demais critérios e definições do Termo de Referência da contratação.
- 1.3. Os Indicadores de Níveis de Serviços serão medidos e avaliados pelo período indicado, tendo como referência o atendimento a chamados de serviço dos diversos tipos e demais indicadores previstos neste documento.
- 1.4. Durante a fase inicial da prestação do serviço, denominado Período de Adaptação Operacional (PAO), conforme previsto no item "6 – Modelo de Execução do Objeto" do Termo de Referência, todos os níveis de serviço serão normalmente apurados e, havendo ocorrência de descumprimento, as glosas serão aplicadas com abatimento de 30% (trinta) em relação ao valor real apurado. Após este período as glosas passam a ser aplicadas integralmente.
- 1.5. Este detalhará os **Indicadores de Níveis de Serviços (INS)**, seus níveis mínimos de serviço (NMS) de desempenho contratuais e suas fórmulas de cálculo.

2. TIPOS DE CHAMADOS DE SERVIÇOS E PRAZOS DE ATENDIMENTO

2.1. Disposições Gerais

- 2.1.1. Durante a vigência das ordens de serviço, solicitações serão encaminhadas à CONTRATADA via chamados de serviço, por meio de ferramenta de ITSM (Information Technology Service Management) da CONTRATANTE, com tipos, categorização e prazos de atendimento específicos.
- 2.1.2. Os chamados podem ser organizados em diferentes tarefas de forma a permitir a organização das atividades e conter o detalhamento de cada uma delas.
- 2.1.3. Solicitações também podem ser recebidas por outros meios, como e-mail

ou chat, nos casos em que a atividade não requer o uso de chamados, como participação em reuniões ou salas de crise.

2.1.4. Na ausência de um chamado de serviço relacionado a uma demanda, é responsabilidade da CONTRATADA realizar o registro apropriado na ferramenta de ITSM da CONTRATANTE, quando aplicável.

2.1.5. Os chamados podem referir-se aos processos ITIL, como Incidentes, Requisições, Mudanças e Problemas, conforme definições presentes neste documento.

2.1.6. Os chamados poderão ser compostos por uma ou mais tarefas, com detalhamentos, responsáveis e prazos específicos.

2.1.7. Para medir a qualidade do serviço, o CONTRATANTE utilizará uma ferramenta informatizada específica de sua propriedade, alinhada às melhores práticas do framework ITIL.

2.1.8. A medição dos serviços apurará o afastamento dos Indicadores de Níveis Serviços em relação às metas estabelecidas.

2.1.9. Os chamados devem ter seus campos preenchidos de forma clara para entender o ocorrido e as ações realizadas para seu atendimento, não sendo aceitas informações genéricas.

2.1.10. A CONTRATADA não poderá suspender o prazo de atendimento na ferramenta de ITSM para atender a outros chamados, em nenhuma hipótese, salvo em situações excepcionais, mediante autorização prévia e expressa da Equipe de Fiscalização do Contrato.

2.1.11. As informações dos chamados de serviço serão importadas para a Base de Conhecimento do CONTRATANTE, sendo responsabilidade da CONTRATADA preencher adequadamente as informações pertinentes ou complementar o preenchimento desta base quando necessário.

2.1.12. A responsabilidade pelo atendimento aos chamados será da CONTRATADA.

2.1.12.1. A CONTRATANTE, contudo, poderá, a seu critério, assumir a responsabilidade pelo tratamento de chamados, situação em que os chamados serão associados a Servidores do Órgão na ferramenta e excluídos do universo amostral de apuração dos resultados da CONTRATADA.

2.1.13. O detalhamento aqui apresentado reflete a maturidade atual dos processos de TIC do órgão, podendo ser atualizado a critério do CONTRATANTE, conforme necessidades específicas e amadurecimento de seus processos.

2.1.14. Os chamados terão prazos para serem recepcionados pelo time responsável por seu tratamento e para a conclusão de seus atendimentos.

2.1.15. Independentemente do escalamento entre os diferentes níveis de atendimento sob responsabilidade da CONTRATADA, o chamado deve atender globalmente os tempos máximos estabelecidos para incidentes e requisições de serviço.

2.1.16. No caso de descumprimentos em relação aos prazos associados aos chamados de serviço, a CONTRATADA terá o prazo de até 5 (cinco) dias úteis após a violação para apresentar as justificativas, tendo a CONTRATANTE até a reunião de acompanhamento. Esta previst no item "6 - Modelo de Execução do Objeto" do Termo de Referência da presente contratação, para avaliar as referidas justificativas.

2.1.17. O catálogo de serviços no "Apêndice II - Catálogo de Serviços" lista os tipos de chamados padronizados atualmente previstos, sendo um documento

dinâmico sujeito a atualizações.

2.1.18. O atendimento às ordens de serviço que são objeto desta contratação deverá levar em consideração, como referência inicial, o atendimento aos requisitos. É resultado esperado desta contratação a redução do volume bruto de chamados de suporte, especialmente no tocante aos incidentes na infraestrutura de TIC, a partir da melhoria da gestão e do aprimoramento dos métodos proativos.

2.2. **Critérios de priorização dos chamados**

2.2.1. Os incidentes, requisições e problemas serão classificados de acordo com os critérios estabelecidos pelo CONTRATANTE, considerando-se: impacto, urgência e prioridade.

2.2.2. Os critérios definidos nas tabelas dos itens 2.3.1 e 2.4.1 a seguir são balizadores para a categorização dos chamados na Ferramenta de Requisição de Serviço e Gerenciamento de TI (ITSM).

2.2.3. O Catálogo de Serviços de TIC, “Apêndice II - Catálogo de Serviços”, vincula cada atendimento presente no catálogo com um determinado grau de impacto.

2.2.4. Os sistemas e recursos de TI a serem suportados pela CONTRATADA estão previstos no “Apêndice I - Infraestrutura de TIC”, e terão os requisitos de urgência/criticidade para cada sistema ou recurso definidos com base nos critérios estabelecidos neste documento.

2.2.5. As classificações de "impacto" e "urgência" poderão ser revistas, assim como poderão ser incluídos novos itens no catálogo de serviços ou na relação de sistemas e recursos de TI, de acordo com a necessidade da CONTRATANTE.

2.2.6. Sempre que a requisição de serviço puder ser agendada para data posterior, ela deverá ter o "impacto" e a "urgência" definidos como "baixos", e deverá ser definida na Ferramenta de Requisição de Serviço e Gerenciamento de TI (ITSM) uma data para sua execução.

2.2.7. A fim de criar um limitador do esforço máximo necessário para o cumprimento dos níveis mínimos de serviços, as requisições classificadas como de prioridades "1" e "2" somadas não poderão exceder a 70% (setenta por cento) das solicitações de incidentes e requisições do período mensal.

2.2.8. Caso os chamados classificados com prioridades "1" e "2" excedam o limite máximo de 70% das solicitações de incidentes e requisições em um determinado mês, não será observado pela CONTRATANTE o acordo de nível de serviço correspondente no que exceder o limite (em ambos os casos será observado o acordado para as prioridades "3 e 4").

2.3. **Impacto**

2.3.1. O impacto reflete o efeito de uma requisição ou incidente sobre o negócio de TI do CONTRATANTE. A classificação dos incidentes, requisições e problemas quanto ao impacto será determinada pela abrangência do incidente e a quantidade de pessoas afetadas:

IMPACTO	FATOS DETERMINANTES
---------	---------------------

ALTO	Incidentes que causem impacto negativo generalizado, e que prejudiquem a imagem institucional do CONTRATANTE; Qualquer incidente relativo à indisponibilidade ou mau funcionamento generalizado de sistemas ou recursos críticos ou essenciais; Qualquer incidente cujo não atendimento comprometa os serviços de TI prestados à população; Incidentes que impeçam ou inviabilizem os trabalhos de uma área ou unidade da organização; Qualquer incidente ou requisição reportado por usuário VIP.
MÉDIO	A falha impossibilita o trabalho diário de um ou mais usuários (ex. problema em um equipamento ou sistema específico, falha no funcionamento do acesso à rede em uma sala ou setor, indisponibilidade da estação de trabalho do usuário, problema em serviço essencial para o usuário); O equipamento ou serviço fornecido está operacional, mas apresenta algumas funções principais, ou partes delas, com erros, provocando assim uma queda na qualidade do trabalho normal.
BAIXO	A falha afeta o trabalho diário de um ou mais usuários; O equipamento ou serviço de uso coletivo encontra-se operando de modo normal, mas algumas funções secundárias apresentam falhas ou lentidão; Trata-se de requisição de serviço cujo não atendimento imediato não impeça o trabalho principal do usuário; A requisição pode ser atendida em algum horário posterior sem que haja prejuízo do desempenho das atividades do usuário.

2.4. Urgência

2.4.1. A urgência é determinada pela necessidade da instituição de que os serviços sejam restabelecidos dentro de um determinado prazo. Serviços e recursos de TI distintos têm requisitos de urgência distintos, dependendo da sua relevância para a missão institucional. A urgência também é determinada pelo aumento da gravidade do incidente, caso não haja atendimento em curto prazo.

IMPACTO	FATOS DETERMINANTES
ALTO	O equipamento ou o serviço precisa ser restabelecido imediatamente; O dano ou o impacto causado pela falha aumenta significativamente com o tempo; O sistema ou recurso é crítico ou essencial; Qualquer incidente ou requisição reportado por usuário VIP.

MÉDIO	O equipamento ou o serviço precisa ser restabelecido o mais rápido possível. Definido para usuários comuns.
BAIXO	O equipamento ou o serviço deve ser restabelecido assim que possível; Por necessidade do cliente não há possibilidade de intervenção imediata; O serviço pode ser agendado para uma data específica, a posteriori.

2.5. Prioridade

2.5.1. A prioridade estabelece a relação de ordem de atendimento dos chamados, nos quais as requisições e incidentes devem ser resolvidos e atendidos. Ela definirá o prazo para início de atendimento e é um importante balizador do esforço a ser empreendido no atendimento.

2.5.2. A partir das classificações de impacto e urgência, e do cruzamento destas informações, é determinada a prioridade de cada requisição e incidente, de acordo com a tabela abaixo:

IMPACTO	URGÊNCIA		
	BAIXA	MÉDIA	ALTA
ALTO	3	2	1
MÉDIO	3	2	2
BAIXO	4	3	3

2.6. Definição de Usuários Vips

2.6.1. A classificação de usuários VIP fundamenta-se na ocupação de cargos de liderança na estrutura organizacional. São considerados usuários VIP os ocupantes dos seguintes cargos: Ministro, Secretários, Diretores, Subsecretários, Ouvidor-Geral, Corregedor-Geral, Assessores Especiais e Assessores do Ministro e de Diretores e Chefes de Gabinete.

2.6.2. Os usuários classificados como VIP deverão registrar suas solicitações diretamente na ferramenta de ITSM ou, alternativamente, designar terceiros, formalmente, para realizarem a abertura dos chamados em seu nome.

2.6.3. Todos os chamados, sejam incidentes ou requisições, originados por usuários VIP deverão, obrigatoriamente, ter o impacto e a urgência classificados como altos, independentemente da natureza do serviço demandado.

2.7. Tipos de chamados

2.7.1. Chamados do tipo Requisição

2.7.1.1. Um chamado de requisição de serviço é uma solicitação formal realizada por um usuário para obter algo previamente autorizado ou previsto no catálogo de serviços da CONTRATANTE. Diferente do incidente, ela não está associada a uma falha ou interrupção, mas sim a uma necessidade rotineira e programada, como fornecimento de acessos, equipamentos ou informações.

2.7.1.2. O gerenciamento de requisições visa fornecer uma experiência eficiente, padronizada e previsível ao usuário, permitindo que demandas recorrentes sejam atendidas com agilidade e, quando possível, de forma automatizada.

2.7.1.3. Entre os exemplos mais frequentes de requisições estão: solicitação de

criação de contas de usuário, instalação de softwares homologados, alteração de senhas, pedidos de acesso a pastas ou sistemas e fornecimento de equipamentos como notebooks ou monitores.

2.7.1.4. Os prazos de recepção e de atendimento das requisições serão contabilizados em horas úteis, a partir do seu registro na ferramenta de ITSM da CONTRATANTE. Isto é, os prazos apenas serão contabilizados dentro da janela padrão da Categoria de Serviço responsável pelo seu atendimento.

2.7.2. Chamados do tipo Incidente

2.7.2.1. Um chamado do tipo incidente é definido, conforme as boas práticas do ITIL v4, como qualquer evento que resulte em uma interrupção não planejada ou redução significativa na qualidade de um serviço de TI. Isso inclui desde falhas completas até degradações de desempenho que impactem a experiência do usuário ou o funcionamento normal das operações.

2.7.2.2. Os chamados de incidentes serão registrados por usuários dos serviços de TIC ou automaticamente por ferramentas específicas do ambiente da CONTRATANTE.

2.7.2.3. Eventos detectados sem chamados de incidentes associados devem ser registrados manualmente pela CONTRATADA para tratamento pelas equipes responsáveis.

2.7.2.4. Causas da não abertura de incidentes para alarmes ou eventos devem ser investigadas, ajustando-se as ferramentas de monitoramento para viabilizar aberturas automáticas.

2.7.2.5. O objetivo principal do gerenciamento de incidentes é restaurar a operação normal do serviço o mais rapidamente possível, minimizando o impacto sobre o negócio. A prioridade de tratamento de um incidente é determinada com base em dois critérios principais: impacto e urgência. É importante destacar que o foco aqui não é descobrir a causa-raiz da falha, mas sim restabelecer o serviço.

2.7.2.6. Exemplos comuns de incidentes incluem sistemas indisponíveis, falhas de rede, erros de autenticação, problemas com impressão, lentidão em aplicações corporativas, ou falhas no envio e recebimento de e-mails. Esses chamados devem ser registrados detalhadamente na ferramenta de ITSM, com atualização constante sobre o andamento da resolução, garantindo comunicação efetiva com o usuário afetado.

2.7.2.7. A contabilização do prazo de encerramento dos incidentes poderá se dar em horas corridas ou horas úteis. Esta definição se baseará em critérios definidos pela CONTRATANTE, como por exemplo a prioridade e o impacto do incidente, e esta informação constará nos chamados.

2.7.3. Chamados escalados de Incidentes para Problemas

2.7.3.1. Um Incidente é definido como uma interrupção não planejada ou uma redução na qualidade de um serviço de TI. Já o Problema refere-se à existência de um erro cuja causa é desconhecida ou à recorrência de um incidente previamente conhecido. Quando a causa de um ou mais incidentes não é identificada, ela será classificada como Problema.

2.7.3.2. O principal objetivo do gerenciamento de problemas é resolver as causas dos incidentes de forma definitiva, minimizando a probabilidade de sua ocorrência novamente. Além disso, busca-se implementar soluções temporárias (**workarounds**) até que a causa raiz seja corrigida permanentemente.

2.7.3.3. Caso a razão de um incidente não seja conhecida, ou nos casos de recorrência de incidentes similares que impactem diversos usuários, ou quando a

abrangência do incidente exceder a necessidade individual do solicitante, deverá ser acionada a Categoria de Serviços de Qualidade, Governança e Melhoria Contínua da Infraestrutura de TIC.

2.7.3.4. Um chamado classificado inicialmente como Incidente só poderá ser escalado para Problema após a validação do CONTRATANTE da apresentação de uma proposta de solução, incluindo a avaliação de impacto e o cronograma de execução fornecidos pela CONTRATADA.

2.7.3.5. Durante a análise de um Problema, é possível que haja uma reclassificação da prioridade do incidente originalmente reportado. Caso um problema esteja relacionado a diversos incidentes ainda abertos, os chamados poderão ser encerrados de forma agrupada, uma vez que o problema tenha sido resolvido. Nesse caso, o nível de serviço deverá ser monitorado e cumprido em relação ao encerramento do Problema.

2.7.4. **Requisições de Mudanças**

2.7.4.1. As mudanças no ambiente computacional serão formalizadas por meio de Requisições de Mudanças (RDMs) a serem submetidas pelas áreas de TI da CONTRATANTE, acompanhadas e geridas pelo Líder do Processo da CONTRATADA e aprovadas (finalizadas) formalmente pela área competente do CONTRATANTE, e devem estar em conformidade com as práticas da biblioteca ITIL 4 ou versão superior.

2.7.4.2. As Requisições de Mudanças devem ser implementadas com níveis adequados de segurança, eficiência e efetividade. Considerando que as tarefas que compõem as RDMs serão passíveis de previsão e planejamento ajustado à capacidade da CONTRATADA, bem como as janelas de manutenções do CONTRATANTE, as atividades ou tickets que compõem os planos terão sempre indicadores de máxima severidade ou máximo impacto.

2.7.4.3. As mudanças devem ser executadas nos horários definidos e autorizados pela CONTRATANTE (janelas de mudança), e previamente acordadas com as áreas solicitantes ou de negócio (área fim) e com a CONTRATADA, pois podem envolver intermitências e indisponibilidades no ambiente de TIC. Vale ressaltar que durante o período registrado das mudanças não devem ser contabilizados os tempos para apuração de disponibilidade nos serviços ou ativos registrados.

2.7.4.4. Quando o CONTRATANTE demandar a execução de Requisição de Mudança, a CONTRATADA deverá apresentar uma proposta de execução destas atividades com a avaliação de impacto, criação de cronograma, monitoramento e controle do processo de mudança.

2.7.4.5. O Tempo Máximo para Solução das Requisições de Mudanças será definido pelo CONTRATANTE, cabendo à CONTRATADA propô-lo, inicialmente, onde incidirão glosas conforme as definidas na tabela de Termo de Serviço (TRS).

2.7.4.6. Não fazem parte do escopo das Requisições de Mudanças a execução de tarefas corriqueiras ou repetitivas pelas áreas especializadas, que não dependam de um planejamento prévio.

2.7.4.7. As RDMs Planejadas têm por objetivo o atendimento de eventuais demandas/necessidades da CONTRATANTE, que podem ser caracterizadas por melhoria no ambiente, manutenção dos procedimentos de trabalho da CONTRATANTE, evolução e/ou implantação de Itens de Configuração que constituem um serviço de infraestrutura de TI.

2.7.4.8. Vale ressaltar ainda que as RDMs envolvem as diversas áreas e atividades de infraestrutura de TIC, incluindo: instalação de novas versões de

sistemas (deploy), trocas de componentes e recursos de hardware, alterações de Domain Names (DNSs), atualizações de certificados, backup e restore de banco de dados (dumps), mudança volumosa de locais de desktops, atualizações nas Aplicações, organização de ambiente do Data Center, readequação de recursos de virtualização, implantação de certificado para aplicações, criação de ambiente para atender a uma aplicação ou unidade, apoio na troca de equipamentos de switches e firewalls, upgrade e migração de SGBDs (Sistemas Gerenciadores de Banco de Dados), criação de repositório de arquivos, implementação do catálogo de softwares e rotinas da atualização de softwares, migração de caixas de e-mail, entre outros.

2.7.4.9. Ao final da execução das Requisições de Mudanças pela CONTRATADA, esta deverá realizar a atualização no Configuration Management Data Base (CMDB) \ Banco de dados do Gerenciamento de Configuração, dos Itens de Configuração (ICs) modificados ou incluídos, bem como atualizar a relação entre os ICs, caso a mudança venha a afetá-los. A não atualização do CMDB pela CONTRATADA implicará em falta e ensejará a aplicação das penalidades previstas.

2.7.4.10. A CONTRATADA deverá realizar verificação da qualidade dos serviços gerados antes de sua entrega, cabendo ao CONTRATANTE também realizar a verificação da qualidade com vistas ao aceite dos produtos.

2.7.4.11. Mesmo uma demanda de serviço já fechada poderá ser objeto de auditoria pelo CONTRATANTE ou a seu comando e, no caso de observadas incorreções, será aberta nova demanda de serviço, para ajustes nos produtos e serviços entregues. Esses registros serão realizados em relatório de auditoria a ser anexado à nova demanda de serviço.

2.7.4.12. A CONTRATADA, para toda demanda de serviço recebida, deverá gerar os artefatos encomendados de acordo com os respectivos cronogramas, entregando produtos dentro dos padrões de qualidade e de compatibilidade técnica, conforme as metodologias, procedimentos, métodos e padrões do CONTRATANTE ou por ele indicados.

2.7.4.13. Em hipótese alguma a CONTRATADA poderá justificar o não atendimento satisfatório dos níveis de serviços mínimos dos demais serviços por estar executando atividades no âmbito de qualquer Requisição de Mudança.

2.7.4.14. A CONTRATADA deverá propor, mensalmente, melhorias no ambiente da CONTRATANTE por meio do Relatório de Execução de Requisições de Mudanças, ou sempre que julgar necessário, com o objetivo de fomentar a adoção das melhores tecnologias disponíveis no mercado.

2.7.4.15. Sempre que considerar necessária a execução planejada de uma atividade, a CONTRATADA poderá sugerir e apresentar um plano de ação para sua realização no período mensal subsequente, o qual estará sujeito à aprovação prévia do CONTRATANTE. Caso o plano seja aprovado, caberá ao CONTRATANTE formalizar a autorização mediante a criação de uma demanda de serviço.

2.7.4.16. Na hipótese de o plano não ser aprovado, a CONTRATADA deverá realizar os ajustes solicitados até que o mesmo atenda aos critérios estabelecidos pelo CONTRATANTE e obtenha sua aprovação. O plano de execução deverá conter o detalhamento das tarefas a serem realizadas, a designação dos responsáveis por cada atividade, bem como as respectivas datas previstas de início e término.

2.7.4.17. Durante a execução mensal, todas as atividades relacionadas às Requisições de Mudança deverão ser devidamente registradas na ferramenta de Requisição de Serviço e Gerenciamento de TI (ITSM), garantindo rastreabilidade, controle e transparência no processo.

2.7.4.18. **Tipos de Mudanças - As RDMs são divididas em três tipos,**

compreendidas da seguinte forma:

I - Mudança Planejada:

- Qualquer mudança nos Serviços de TIC e outros Itens de Configuração, que não se enquadre como uma mudança do tipo padrão ou emergencial.
- A RDM do tipo **Planejada** deve incluir todos os requisitos necessários para sua execução e ser discutida e aprovada pelas áreas responsáveis pela **Infraestrutura de TI** da CONTRATANTE que serão impactadas pela mudança.
- A execução da RDM deverá ocorrer exclusivamente fora do horário de expediente (após às 20h ou aos finais de semana), conforme as **janelas de manutenção** previamente estabelecidas pelo CONTRATANTE.

II - Mudança Emergencial:

- Toda mudança que for registrada visando sua execução fora dos dias e horas do Calendário de Mudança Planejada, sendo que as RDMs podem ser registradas posterior ou em paralelo a execução da Mudança.
- A RDM emergencial se enquadra nas seguintes situações: uma mudança for necessária para a resolução de indisponibilidade nos Serviços de TIC ou em um ou mais Itens de Configuração (ICs), devendo ser executada imediatamente ou o quanto antes, dentro ou fora do horário de expediente;
- São exemplos de situações que demandam RDMs Emergenciais: quando a execução da mudança estiver relacionada à possibilidade de perdas financeiras significativas para a CONTRATANTE; quando a necessidade de implementar a mudança envolver grandes danos ou impactos negativos à imagem da CONTRATANTE; ou quando a mudança for necessária para corrigir erros em funcionalidades de Serviços de TIC e outros Itens de Configuração que estejam prejudicando a prestação de serviços públicos.

III - Mudança Padrão:

- Uma mudança padrão tem como objetivo simplificar o processo de análise, aprovação e execução das requisições, caracterizando-se como uma mudança pré-aprovada e de baixo risco. Esse tipo de mudança visa otimizar o tempo e os recursos, permitindo sua execução de maneira ágil e sem a necessidade de avaliações complexas a cada solicitação.
- Para que uma mudança seja classificada como "padrão", ela deve atender aos seguintes requisitos: primeiramente, deve ter sido executada pelo menos uma vez como "Planejada", passando por uma revisão pós-implementação, sendo considerada realizada com sucesso e sem ressalvas. Além disso, os horários de execução da mudança são pré-estabelecidos pelo CONTRATANTE, podendo ocorrer tanto dentro quanto fora do horário de expediente, conforme as necessidades do negócio.

- As atividades relacionadas à mudança padrão devem ser idênticas às realizadas anteriormente, com tempos de execução semelhantes. Ademais, é necessário que exista um modelo de mudança previamente definido, aprovado e configurado na ferramenta de ITSM. Mudanças consideradas de baixo risco, simples e rotineiras, que são frequentemente executadas, poderão ser classificadas como padrão desde que sejam apresentadas e aprovadas pelas áreas responsáveis de Infraestrutura de TIC e do Negócio impactadas.

2.8. Prazos de Atendimento

2.8.1. O tempo de início de tratamento do chamado (TIT) é o tempo transcorrido desde o registro do chamado na ferramenta de requisição de serviço e gerenciamento de TI (ITSM) por um usuário, por uma ferramenta automatizada ou pela própria CONTRATADA, até a sua atribuição no próprio sistema à área responsável, com início imediato da contagem do tempo de atendimento do incidente ou requisição, independentemente de o atendimento ser realizado de forma presencial ou de forma remota.

2.8.2. No caso da requisição do serviço ou incidente ser feita por chamada telefônica ou por e-mail, o TIT é o intervalo entre o início do atendimento pelo atendente e a consequente geração do número do chamado até a efetiva designação de um colaborador para o atendimento dos incidentes e requisições (que poderá ser o próprio atendente, no caso de resolução do problema em primeiro nível).

2.8.3. O registro do "TIT" é, portanto, de responsabilidade exclusiva do atendimento remoto na Central de Serviços. No caso do atendimento via telefone ou por e-mail, deverão ser desconsideradas as estatísticas das chamadas inconclusas ou que não obtiverem êxito em transmitir completamente as informações relativas ao problema.

2.8.4. O Tempo Máximo para Solução do Incidente (TMSI) é o tempo máximo para a resolução de um incidente, contado do momento da atribuição do chamado pela Central de Serviço a uma determinada categoria de serviço até o encerramento no sistema de ITSM.

2.8.5. O Tempo Máximo para Solução da Requisição (TMSR) é o tempo máximo para a resolução de uma requisição, contado do momento da atribuição do chamado pela Central de Serviço a uma determinada categoria de serviço até o encerramento no sistema de ITSM.

2.8.6. No que diz respeito ao atendimento das categorias de serviço sem previsão de cobertura 24x7, o tempo transcorrido fora da janela de atendimento prevista no item 2.4.1 do presente Termo de Referência, não será considerado para efeito do cálculo do TMSI e do TMSR.

2.8.7. O Tempo Máximo para Solução da Requisição de Mudança Planejada (TMSRMP) é o tempo acordado no cronograma proposto pelo CONTRATANTE e aceito pela CONTRATADA. O controle dessas requisições será realizado por meio dos Termos de Serviços.

2.8.8. Os prazos máximos para início do tratamento e de solução dos incidentes ou requisições, de acordo com o nível de prioridade de atendimento, estão descritos na tabela abaixo, desde que a solução da requisição ou tratamento do incidente dependa exclusivamente da CONTRATADA.

Tabela de Tempo Máximo por Prioridade de Atendimento

PRIORIDADE	TEMPO DE INÍCIO DE TRATAMENTO DO CHAMADO (TIT)	INCIDENTES	REQUISIÇÕES	REQUISIÇÕES PLANEJADAS
		TEMPO MÁXIMO PARA SOLUÇÃO DO INCIDENTE (TMSI)	TEMPO MÁXIMO PARA SOLUÇÃO DA REQUISIÇÃO (TMSR)	TEMPO MÁXIMO PARA SOLUÇÃO DA REQUISIÇÃO DE MUDANÇA PLANEJADA (TMSRMP)
1 - Muito Alta	Em até 15 min	Em até 1h	Em até 2h	De acordo com o Cronograma proposto pelo CONTRATANTE e aceito pela CONTRATADA
2 - Alta	Em até 15 min	Em até 2h	Em até 4h	
3 - Média	Em até 15 min	Em até 4h	Em até 8h	
4 - Baixa	Em até 15 min	Em até 8h	Em até 16h	

2.9. Qualidade dos produtos e Serviços

2.9.1. Com o objetivo de assegurar o padrão de qualidade exigido pelo CONTRATANTE, a CONTRATADA deverá:

I - Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos e ferramentas;

II - Fiscalizar regularmente os seus recursos técnicos designados para a prestação dos serviços verificando as condições em que as atividades estão sendo realizadas;

III - Refazer todos os serviços que, a juízo do representante do CONTRATANTE, de forma fundamentada, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado, independentemente das penalidades previstas;

IV - Efetuar adequação das instalações e procedimentos realizados quanto à eficiência, eficácia, ocorrência de reincidência, segurança, conformidade com as boas práticas e normas aplicáveis.

V - Adequar a redação de documentos e relatórios quanto à clareza, objetividade, detalhamento técnico e conformidade com as boas práticas e normas aplicáveis.

VI - Executar fielmente o objeto contratado de acordo com as normas legais, em conformidade com a proposta apresentada e com as orientações do CONTRATANTE, observando sempre os critérios de qualidade.

2.9.2. A CONTRATADA deverá criar mecanismos para realizar enquetes ou pesquisas de satisfação, através do portal de autoatendimento web, ou ainda por correio eletrônico ou por programação do sistema telefônico. As respostas deverão ser enviadas à base de dados da ferramenta de requisição de serviço e gerenciamento de TI (ITSM).

2.9.3. A CONTRATADA deverá armazenar todos os resultados das pesquisas de satisfação para a geração de relatórios e dashboards.

2.9.4. Os relatórios de pesquisa de satisfação serão utilizados como insumo

para medição do Índice de Satisfação do Atendimento ao Usuário, entre os valores 1 (totalmente insatisfeito) até 5 (totalmente satisfeito).

2.9.5. As pesquisas deverão ser realizadas de forma compulsória, podendo ou não utilizar algum mecanismo de amostragem, e o CONTRATANTE poderá também definir junto à CONTRATADA a realização de pesquisas em momentos específicos.

2.10. **Base de conhecimento**

2.10.1. O registro, uso, manutenção e reuso de conhecimento deve ser prática comum da CONTRATADA.

2.10.2. Todos os incidentes devem ser relacionados a um conhecimento, o qual pode ser um Incidente anterior, um artigo de conhecimento da ferramenta de gerenciamento de serviços de TIC (ITSM), um link web para uma página de documentação criada especificamente para esse fim ou outro meio estipulado pela CONTRATANTE.

2.10.3. Caso o conhecimento ainda não exista, a CONTRATADA terá uma tarefa de incidente associada com prazo de 3 (três) dias úteis para criar o conhecimento e associá-lo ao Incidente.

2.10.4. Os Incidentes semelhantes devem ser associados ao mesmo conhecimento.

3. **INDICADORES DE NÍVEIS DE SERVIÇOS**

3.1. Para permitir que a gestão contratual esteja alinhada com a gestão da qualidade dos serviços prestados, foram estabelecidos Indicadores de Níveis de Serviços (INS) para a medição da execução dos serviços contratados.

3.2. A Portaria SGD/MGI nº 1.070/2023, define:

12.2.9. Relaciona-se a seguir o conjunto mínimo de indicadores proposto para o presente modelo, pautado no incentivo para a redução de ocorrências que impactam o negócio do contratante e também incentivem a boa prestação dos serviços contratados:

- a) Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo
- b) Disponibilidade de um ambiente/serviço
- c) Eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança)
- d) Satisfação dos usuários
- e) Índice de vinculação da resolução de requisições de serviço à base de conhecimento

3.2.1. No que diz respeito à proposta de INS para "Disponibilidade de um ambiente/serviço", este foi dividido em dois INSs: (1) "Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Críticos"; e (2) "Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Essencial"

3.3. Assim, os resultados serão medidos com base em indicadores vinculados a fórmulas de cálculo específicas, apurados temporalmente e continuamente monitorados, objetivando o cumprimento das metas estabelecidas.

3.4. Esse conceito vincula-se ao novo modelo de contratação de soluções de Tecnologia da Informação na Administração Pública Federal, no qual os serviços serão remunerados considerando parâmetros de qualidade e entrega efetiva de resultados.

3.5. Os atendimentos aos usuários de TI estão definidos em um Catálogo de Serviços, que deverá ser incremental (identificado e preenchido constantemente).

Ou seja, os novos serviços identificados pela CONTRATADA deverão ser implementados e entregues a CONTRATANTE.

3.6. No Catálogo de Serviços estão relacionadas as categorias de serviços que os usuários de Tecnologia da Informação podem receber atendimento.

3.7. A prestação dos serviços leva ainda em consideração a resposta aos incidentes de TI, sejam eles reportados por usuários ou instaurados automaticamente através de ferramentas de monitoramento.

3.8. Os dados necessários para o cálculo dos indicadores da prestação de serviços de TI serão obtidos exclusivamente da ferramenta de requisição de serviço e gerenciamento de TI (ITSM), no caso dos indicadores de qualidade do atendimento telefônico na Central de Serviços, diretamente da Central de Atendimento da CONTRATADA, e de ferramentas de monitoramento dos serviços, para apuração dos indicadores de disponibilidade.

3.8.1. Como instrumentos de medição serão utilizados os sistemas: de atendimento aos chamados (ferramenta ITSM adotada pela CONTRATANTE), de gerência técnica de serviços de TIC e de monitoramento de redes, servidores e serviços (Zabbix ou similar).

3.9. Para os serviços contratados, serão apurados os seguintes indicadores:

ID do Indicador	INS
INS-01	Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo
INS-02	Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Críticos
INS-03	Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Essencial
INS-04	Eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança)
INS-05	Satisfação dos usuários
INS-06	Índice de vinculação da resolução de requisições de serviço à base de conhecimento
INS-07	Indicador do Plano de Capacitação por categoria de serviço
INS-08	Indicador de implantação contínua de processos automatizados
INS-09	Indicador de redução contínua das vulnerabilidades de segurança
INS-10	Tempo Médio de Resposta Autônoma (MTTA-AI)
INS-11	Taxa de Resolução Autônoma de Incidentes
INS-12	Indicador de Disponibilidade da Plataforma da CONTRATADA

3.10. A seguir o INSs são apresentados em detalhes:

3.10.1. **Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo (INS-01)**

Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo (INS-01)	
Tópico	Descrição

Finalidade	Apurar a quantidade de chamados atendidos dentro do prazo estabelecido
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	Maior ou igual a 99%.
Instrumento de medição	Ferramenta de Monitoramento de ativos de TIC.
Forma de acompanhamento	O acompanhamento será realizado por meio de relatório mensal extraído da ferramenta de Monitoramento de ativos de TIC.
Periodicidade	Mensal
Mecanismo de cálculo (%)	$(\text{Total de chamados atendidos dentro do prazo} / \text{Total de chamados abertos no período}) \times 100$
Início da vigência	A partir do início da efetiva prestação de serviços.
Faixa no ajuste no pagamento	Conforme indicação da tabela do item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Serão utilizados dias corridos na medição.

3.10.2. Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Críticos (INS-02):

Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Críticos (INS-02)	
Tópico	Descrição
Finalidade	Apurar o percentual do tempo em que os serviços e recursos relacionados como críticos estiveram disponíveis no mês.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	Maior ou igual a 99,9%.
Instrumento de medição	Ferramenta de Monitoramento de ativos de TIC.
Forma de acompanhamento	O acompanhamento será realizado por meio de relatório mensal extraído da ferramenta de Monitoramento de ativos de TIC.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	Tempo de disponibilidade de todos os serviços e recursos relacionados como críticos, dividido pelo tempo total de operação de todos os serviços e recursos relacionados como críticos, vezes cem.

Início de Vigência	A partir do início da efetiva prestação de serviços.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Serão utilizados dias corridos na medição.

3.10.3. **Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Essencial (INS-03):**

Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Essencial (INS-03)	
Tópico	Descrição
Finalidade	Apurar o percentual do tempo em que os serviços e recursos relacionados como essenciais estiveram disponíveis no mês.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	Maior ou igual a 99,50%.
Instrumento de medição	Ferramenta de Monitoramento de ativos de TIC.
Forma de acompanhamento	O acompanhamento será realizado por meio de relatório mensal extraído da ferramenta de Monitoramento de ativos de TIC.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	Tempo de disponibilidade de todos os serviços e recursos relacionados como essenciais, dividido pelo tempo total de operação de todos os serviços e recursos relacionados como essenciais, vezes cem.
Início de Vigência	A partir do início da efetiva prestação de serviços.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Serão utilizados dias corridos na medição.

3.10.4. **Eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança) - (INS-04)**

Eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança) - (INS-04)	
Tópico	Descrição
Finalidade	Apurar o percentual de demandas que são reabertas em até 7 dias após a sua conclusão.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	Maior ou igual a 98%.
Instrumento de medição	Ferramenta de ITSM.
Forma de acompanhamento	O acompanhamento será realizado por meio de relatório mensal extraído da ferramenta de ITSM.
Periodicidade	Mensal
Mecanismo de cálculo (%)	$\frac{\text{Total de chamados atendidos} - \text{Total de chamados reaberto em até 7 dias}}{\text{Total de chamados atendidos}} \times 100$ <Consideram-se atendidos os chamados fechados com solução, não devendo ser considerados os chamados fechados sem solução>
Início da vigência	A partir do início da efetiva prestação de serviços.
Faixa no ajuste no pagamento	Conforme indicação da tabela do item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Consideram-se concluídos os chamados que foram atendidos e encerrados na ferramenta de ITSM com a sua respectiva solução. Serão utilizados dias corridos na medição.

3.10.5. Satisfação dos usuários (INS-05)

Satisfação dos usuários (INS-05)	
Tópico	Descrição
Finalidade	Aferir o grau de satisfação dos usuários sobre o serviço prestado
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	Média maior ou igual a 4 pontos .
Instrumento de medição	Ferramenta de ITSM.
Forma de acompanhamento	O acompanhamento será realizado por meio de relatório mensal extraído da ferramenta de ITSM.
Periodicidade	Mensal

Mecanismo de cálculo (%)	(Média das notas obtidas) / (Nota máxima da avaliação)
Início da vigência	A partir do início da efetiva prestação de serviços.
Faixa no ajuste no pagamento	Conforme indicação da tabela do item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação.
Observações	A escala de avaliação para cada chamado será de 1 (totalmente insatisfeito) até 5 (totalmente satisfeito). Chamados com avaliação de 1 (totalmente insatisfeito) serão penalizados conforme Termo de Serviço. Escala: () totalmente satisfeito (Nota 5); () satisfeito (Nota 4); () nem satisfeito nem insatisfeito (Nota 3); () insatisfeito (Nota 2); () totalmente insatisfeito (Nota 1). Serão utilizados dias corridos na medição.

3.10.6. Índice de vinculação da resolução de requisições de serviço à base de conhecimento (INS-06)

Indicador de vinculação da resolução de requisições de serviço à base de conhecimento (INS-06)	
Tópico	Descrição
Finalidade	Aferir a cobertura dos padrões de atendimento registrados na base de conhecimento.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	Maior ou igual a 99,50%.
Instrumento de medição	Ferramenta de ITSM.
Forma de acompanhamento	O acompanhamento será realizado por meio de relatório mensal extraído da ferramenta de ITSM.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	Total de requisições com resolução vinculada à base de conhecimento / Total de requisições resolvidas x 100
Início de Vigência	A partir do início da efetiva prestação de serviços.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação

Observações	Serão utilizados dias corridos na medição. Serão contabilizados chamados do tipo requisição e incidente.

3.10.7. Indicador do Plano de Capacitação por categoria de serviço (INS-07):

Indicador do Plano de Capacitação por categoria de serviço (INS-07)	
Tópico	Descrição
Finalidade	Promover a capacitação da equipe utilizada na prestação dos serviços nas áreas de interesse da contratação.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	No mínimo 8 Cursos ou treinamentos
Instrumento de medição	Relatório gerenciais dos serviços com os respectivos comprovantes dos cursos e treinamentos.
Forma de acompanhamento	Acompanhamento dos relatórios gerenciais dos serviços.
Periodicidade	Será aferido a cada 12 meses
Mecanismo de Cálculo (métrica)	A Contratada deverá realizar, no mínimo, 8 certificações ou treinamentos oficiais por ano e registrar esta informação mensalmente, de forma acumulativa, nos relatórios gerenciais de serviço, conforme presente Termo de Referência da presente contratação..
Início de Vigência	A partir do início da efetiva prestação de serviços.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Serão utilizados dias corridos na medição.

3.10.8. Indicador de implantação contínua de processos automatizados (INS-08):

Indicador de implantação contínua de processos automatizados (INS-08)	
Tópico	Descrição
Finalidade	Apurar a automação dos processos identificados como passíveis de automação que ainda não tenham sido automatizados durante o período de 12 meses.

Meta a cumprir (Níveis Mínimos de Serviços - NMS)	Automatização de 50% dos processos identificados como passíveis de automação que ainda não tenham sido automatizados.
Instrumento de medição	Relatório gerenciais dos serviços.
Forma de acompanhamento	O acompanhamento dos relatórios gerenciais dos serviços.
Periodicidade	Será aferido a cada 12 meses.
Mecanismo de Cálculo (métrica)	A contratada deverá, a cada doze meses, automatizar ao menos 50% dos processos identificados como passíveis de automação que ainda não tenham sido automatizados.
Início de Vigência	A partir da definição do escopo de processos identificados como passíveis de automação definidas pela CONTRATANTE.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Serão utilizados dias corridos na medição.

3.10.9. Indicador de redução contínua das vulnerabilidades de segurança (INS-09):

Indicador de redução contínua das vulnerabilidades de segurança (INS-09)	
Tópico	Descrição
Finalidade	Apurar a efetividade na correção de vulnerabilidades de segurança identificadas por meio das ferramentas do CONTRATANTE.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	Redução de 70% da quantidade de vulnerabilidades de segurança identificadas por meio das ferramentas do CONTRATANTE.
Instrumento de medição	Ferramentas de segurança utilizadas pela CONTRATANTE.
Forma de acompanhamento	O acompanhamento dos relatórios das ferramentas de segurança utilizadas pela CONTRATANTE e dos relatórios gerenciais dos serviços.
Periodicidade	Será aferido a cada 12 meses.
Mecanismo de Cálculo (métrica)	A contratada deverá, a cada doze meses, reduzir ao menos em 70% a quantidade de vulnerabilidades de segurança identificadas por meio das ferramentas do CONTRATANTE.

Início de Vigência	A partir da definição do escopo de vulnerabilidades definidas pela CONTRATANTE.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Serão utilizados dias corridos na medição.

3.10.10. Tempo Médio de Resposta Autônoma (MTTA-AI)

Indicador de Tempo Médio de Resposta Autônoma (MTTA-AI) (INS-10)	
Tópico	Descrição
Finalidade	Mede o tempo médio decorrido entre a detecção de um evento ou incidente e o início da primeira ação automatizada de investigação ou resposta executada pela plataforma.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	O valor do MTTA-AI deverá ser igual ou inferior a 30 (trinta) segundos.
Instrumento de medição	A medição deverá ser realizada por meio de logs auditáveis contendo, no mínimo: timestamp da detecção do evento; timestamp da execução da primeira ação; identificação do incidente;
Forma de acompanhamento	O acompanhamento será realizado por meio de relatório mensal extraído da ferramenta de Monitoramento de ativos de TIC.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	$\text{MTTA-AI} = (\text{somatório de (Tempo de início da ação - Tempo de detecção do evento)}) / \text{número total de incidentes}$
Início de Vigência	A partir do início da efetiva prestação de serviços.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Não poderão ser excluídos da medição: incidentes classificados como críticos ou altos; incidentes com impacto em serviços de produção;

3.10.11. Taxa de Resolução Autônoma de Incidentes

Taxa de Resolução Autônoma de Incidentes (INS-11)	
Tópico	Descrição
Finalidade	Mede o percentual de incidentes resolvidos integralmente pela plataforma sem intervenção humana em qualquer etapa decisória.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	A taxa de resolução autônoma deverá ser igual ou superior a 40% (quarenta por cento) para os primeiros 12 (doze) meses de execução contratual. A taxa de resolução autônoma deverá ser igual ou superior a 45% (quarenta e cinco por cento) para o segundo período de vigência contratual A taxa de resolução autônoma deverá ser igual ou superior a 55% (cinquenta e cinco por cento) a partir dos 30º (trigésimo) mês de execução contratual.
Instrumento de medição	O acompanhamento será realizado por meio de relatório mensal extraído da ferramenta de Monitoramento de ativos de TIC.
Forma de acompanhamento	A validação da resolução deverá considerar: retorno do serviço ao estado normal (baseline); ausência de novos alertas correlacionados em janela mínima configurável; confirmação via sistema de monitoramento ou ITSM integrado; A CONTRATADA deverá manter trilha de auditoria contendo: ações executadas pelo agente de IA; decisões automatizadas; evidências de normalização;
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	$\text{Taxa de Resolução Autônoma (\%)} = (\text{número de incidentes resolvidos automaticamente} / \text{número total de incidentes}) \times 100$
Início de Vigência	A partir do início da efetiva prestação de serviços.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item item 3.11 do presente Apêndice.
Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação

Observações	a) Considera-se “resolução automática” o incidente que: percorreu todo o ciclo de vida sem intervenção humana; foi solucionado por ação automatizada da plataforma; teve a normalização do serviço confirmada por métricas ou monitoramento; b) Não serão considerados como resolvidos automaticamente: incidentes encerrados manualmente; incidentes sem evidência de normalização do serviço; incidentes classificados como informativos ou sem impacto operacional relevante;

3.10.12. **Indicador de Disponibilidade da Plataforma da CONTRATADA**

Indicador de Disponibilidade da Plataforma da CONTRATADA (INS-12)	
Tópico	Descrição
Finalidade	Mede o percentual de tempo em que a plataforma da CONTRATADA permanece disponível e plenamente operacional durante o período de apuração.
Meta a cumprir (Níveis Mínimos de Serviços - NMS)	A disponibilidade da plataforma deverá ser igual ou superior a 99,7% (noventa e nove vírgula sete por cento) ao mês.
Instrumento de medição	A disponibilidade deverá ser apurada com base em: logs de monitoramento; ferramentas independentes de verificação; registros de incidentes;
Forma de acompanhamento	a) Considera-se “tempo de indisponibilidade” qualquer período em que a plataforma esteja: totalmente indisponível; parcialmente indisponível, impossibilitando a execução de funcionalidades essenciais; com degradação severa de desempenho que impeça a operação normal; b) Incluem-se como indisponibilidade: falhas sistêmicas; indisponibilidade de serviços críticos; interrupções não previamente autorizadas;
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	$\text{Disponibilidade (\%)} = ((\text{Tempo total do período} - \text{Tempo de indisponibilidade}) / \text{Tempo total do período}) \times 100$
Início de Vigência	A partir do início da efetiva prestação de serviços.
Faixas de ajuste no pagamento	Conforme indicação da tabela do item item 3.11 do presente Apêndice.

Sanções	Serão aplicadas as sanções previstas na Ocorrência nº 14 da Tabela apresentada no subitem 9.1, da seção "9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO" do Termo de Referência da presente contratação
Observações	Deverão ser excluídas da apuração, desde que previamente aprovadas pela CONTRATANTE:janelas de manutenção programadas; interrupções previamente autorizadas;

3.10.13. Para aferição da qualidade dos serviços executados, serão mensurados mensalmente e monitorados continuamente os indicadores de prestação de serviços de TI vinculados a cada OS, utilizando-se as respectivas fórmulas de cálculo, e segundo as metas (Níveis Mínimos de Serviços - NMS) estabelecidas.

3.11. Os pontos computados pela fiscalização mensal incidirão em glosas, conforme TABELA a seguir, haverá redução de 0,001 (equivalente a 0,1%) sobre o valor do pagamento mensal devido a cada 1 (um) ponto no período de faturamento:

ID do Indicador	INS	PONTUAÇÃO ACUMULÁVEL
INS-01	Quantidade de chamados (requisição e incidentes) atendidos dentro do prazo	10 pontos a cada 0,1% abaixo da meta
INS-02	Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Críticos	10 pontos a cada 0,1% abaixo da meta
INS-03	Indicador de Disponibilidade da Sustentação de Sistemas e Recursos Essencial	10 pontos a cada 0,1% abaixo da meta
INS-04	Eficácia no tratamento de chamados (requisições, incidentes e incidentes de segurança)	10 pontos a cada 0,1% abaixo da meta
INS-05	Satisfação dos usuários	5 pontos a cada 1% abaixo da meta

INS-06	Índice de vinculação da resolução de requisições de serviço à base de conhecimento	1 ponto a cada 0,1% abaixo da meta
INS-07	Indicador do Plano de Capacitação por categoria de serviço	10 pontos a cada 01 Certificação/Treinamento abaixo da meta
INS-08	Indicador de implantação contínua de processos automatizados	1 ponto a cada 1% abaixo da meta
INS-09	Indicador de redução contínua das vulnerabilidades de segurança	1 ponto a cada 1% abaixo da meta
INS-10	Tempo Médio de Resposta Autônoma (MTTA-AI)	1 ponto a cada 1s acima do NMS
INS-11	Taxa de Resolução Autônoma de Incidentes	2 ponto a cada 1% abaixo da meta
INS-12	Indicador de Disponibilidade da Plataforma da CONTRATADA	5 pontos a cada 0,1% abaixo da meta

3.11.1. Conforme disposto no item 12.2.5 da Portaria SGD/MGI nº 1.070/2023, os valores referentes à redução por descumprimento dos Níveis Mínimos de Serviço estão limitados a 30% do valor do faturamento mensal. Caso esse percentual seja excedido, a diferença será descontada no mês subsequente.

"12.2.5. As margens de tolerância se referem a um limite de desconto na fatura mensal (não superior a 30% sobre o valor mensal), cujo eventual saldo devedor (caso ultrapasse o limite mensal preestabelecido) poderá ser aplicado na fatura do mês subsequente, à exceção do último mês de vigência do contrato."

3.12. O Período de Adaptação Operacional (PAO) da CONTRATADA terá a duração de 90 (noventa) dias contados a partir da emissão da primeira Ordem de Serviço contratual.

3.12.1. Durante este período, os níveis de prestação dos serviços de TI e os Termos de Serviço previstos em contrato serão ajustados por um desconto de 30% do valor da glosa.

3.12.2. Com o término do PAO, os níveis mínimos de serviço serão observados integralmente.

3.13. Os níveis de prestação dos serviços de TI mínimos não poderão ser revisados pelo CONTRATANTE, devido à possibilidade de quebra da isonomia do processo licitatório e da perda da vinculação ao instrumento convocatório (Acórdão TCU 717/2010 – Plenário).

4. TERMOS DE SERVIÇOS (TRS)

4.1. Além dos indicadores estabelecidos, serão aplicadas glosas com base

nas pontuações atribuídas ao descumprimento dos termos de serviço, sem prejuízo de outras sanções administrativas por descumprimento das obrigações contratuais. As ocorrências serão apuradas dentro do período de um mês.

4.2. As pontuações referentes aos Termos de Serviço também estarão sujeitas a fatores de redução durante o Período de Adaptação Operacional, bem como ao limite previsto no item 3.12 deste documento.

4.3. Os Termos de Serviço a serem observados pela CONTRATADA, juntamente com suas respectivas penalizações, estão detalhados na tabela a seguir.

Sigla	Assunto	Termo de Serviço	Referência	Pontuação
TRS1	Base de Dados	Deixar de documentar os ICs e de manter completa e atualizada a Base de Dados de Configuração, inclusive no que diz respeito aos diagramas e desenhos.	Por ocorrência	1 ponto
TRS2	Base de Dados	Deixar de produzir ou de manter atualizadas as rotinas e scripts da Base de Dados de Conhecimentos.	Por ocorrência	1 ponto
TRS3	Base de Dados	Deixar de implantar em um prazo de quatro meses após o início da prestação dos serviços link de dados exclusivo entre CONTRATADA e CONTRATANTE, atendendo aos requisitos presentes.	Por mês incompleto de atraso	10 pontos
TRS4	Base de Dados	Perder dados ou informações corporativas por erros na operação devidamente comprovados.	Por ocorrência	10 pontos
TRS5	Chamado	Finalizar a requisição de serviço ou incidente sem a anuência do solicitante ou sem que o mesmo tenha sido solucionado, ou deixar de realizar os testes para aferir a efetiva resolução.	Por ocorrência	1 pontos
TRS6	Chamado	Deixar de notificar incidentes repetitivos, quer tenham sido conhecidos através do monitoramento ou por notificações de usuários, para a Categoria de Serviço de Serviços de Qualidade, Governança e Melhoria Contínua da Infraestrutura de TIC	Por ocorrência	1 ponto
TRS7	Chamado	Deixar de apresentar ao CONTRATANTE o impacto e o cronograma da solução do Problema no Tempo Máximo para Solução do Incidente do respectivo Incidente que deu origem ao Problema.	Por ocorrência	1 ponto
TRS8	Chamado	Deixar de executar a solução de um Problema conforme cronograma definido pelo CONTRATANTE.	Por ocorrência	5 pontos
TRS9	Chamado	Realizar cancelamento de chamado na ferramenta de ITSM sem justificativa aceitável pela CONTRATANTE.	Por ocorrência	1 ponto

TRS10	Chamado	Deixar de atender no triplo do tempo os chamados que não foram solucionados no Tempo Máximo para Solução do Incidente, no Tempo Máximo para Solução da Requisição e no Tempo Máximo para Solução da Requisição Planejada de acordo com o definido na tabela de Tempo de Início e Tempo Máximo por Prioridade de Atendimento.	Por chamado	5 pontos
TRS11	Chamado	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, chamados de requisição e incidentes. Neste item também entrará a "pausa de chamado" injustificada ou indevida.	Por chamado	1 ponto
TRS12	CMDB	Deixar de implementar o CMDB de todos os itens de configuração descritos no documento, integrada à ferramenta ITSM no prazo máximo de 60 dias após o início da prestação do serviço.	Por mês de atraso cumulativo	10 pontos
TRS13	CMDB	Deixar de realizar a atualização no Configuration Management Data Base (CMDB) dos Itens de Configuração (ICs) modificados ou incluídos, bem como atualizar a relação entre os ICs, caso a Requisição Planejada que venha a afetá-los.	Por ocorrência	1 ponto
TRS14	Danos	Causar qualquer dano aos equipamentos do contratante por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	10 pontos
TRS15	Fraude	Fraudar, manipular ou descaracterizar indicadores/metas de níveis de serviço e de desempenho por quaisquer subterfúgios.	Por ocorrência de Indicador Manipulado	10 pontos
TRS16	ITSM	Deixar de configurar durante o PAO a Ferramenta de Requisição de Serviço e Gerenciamento de TI, e a Ferramenta de Suporte Remoto com todas as características e requisitos necessários.	Por mês incompleto de atraso	10 pontos
TRS17	ITSM	Deixar de documentar qualquer ocorrência (incidentes, requisições, mudanças, problemas, indisponibilidades) na Ferramenta de Requisição de Serviço e Gerenciamento de TI (ITSM).	Por ocorrência	5 pontos
TRS18	Monitoramento	Deixar de operar e monitorar proativamente o ambiente de TI, e de atuar tempestivamente no caso de incidentes graves.	Por ocorrência	10 pontos

TRS19	Novas Soluções	Deixar de analisar a viabilidade e o impacto da instalação de novas soluções e correções.	Por ocorrência	5 pontos
TRS20	Obrigações	Deixar de cumprir qualquer outra obrigação estabelecida no edital e não prevista nesta tabela, de forma reincidente, após formalmente notificada pelo CONTRATANTE	Por ocorrência	5 pontos
TRS21	Organização	Deixar de zelar pela organização, acomodação e correta identificação dos cabos nos racks de equipamentos e patch panels, ou não cuidar da correta montagem e conservação dos equipamentos do datacenter e demais unidades de prestação de serviços.	Por ocorrência	5 pontos
TRS22	Política de segurança	Incluir, excluir ou alterar regras dos dispositivos de segurança sem autorização do gestor de TI, ou contrariando as políticas de segurança do CONTRATANTE.	Por ocorrência	10 pontos
TRS23	Política de segurança	Deixar de cumprir ou de implantar as Políticas de Segurança e de Continuidade de Negócios de TI.	Por ocorrência	10 pontos
TRS24	Política de segurança	Permitir que violações de segurança afetem ou causem indisponibilidade dos sistemas do CONTRATANTE, sem aplicar as contramedidas necessárias.	Por ocorrência	10 pontos
TRS25	Política de segurança	Deixar de planejar e instalar nos equipamentos e sistemas as atualizações e patches de segurança disponibilizados pelos fabricantes e distribuidores.	Por ocorrência	10 pontos
TRS26	Política de segurança	Deixar de aplicar as políticas de controle de acesso e de gestão da identidade de usuários de TI.	Por ocorrência	5 pontos
TRS27	Política de segurança	Deixar de realizar os testes e análises de vulnerabilidades e potenciais falhas de segurança, conforme política de segurança da informação.	Por ocorrência	5 pontos
TRS28	Profissionais	Permitir a presença de profissional sem crachá nos locais onde há prestação de serviço para o CONTRATANTE, após reincidência formalmente notificada.	Por ocorrência	1 ponto
TRS29	Profissionais	Não realizar a comunicação imediata nos casos de substituição de perfis profissionais previstos na Ordem de Serviço (OS).	Por ocorrência	1 ponto

TRS30	Profissionais	Deixar de retirar profissional que se conduza de modo inconveniente, que não respeite as normas do CONTRATANTE ou que não atenda às necessidades, em no máximo 24 horas após a notificação formal.	Por ocorrência	1 ponto por dia incompleto que exceder as 24 horas
TRS31	Profissionais	Deixar de alocar perfil profissional previsto na Ordem de Serviço durante o período de medição mensal dos Serviços.	Por ocorrência	10 pontos para cada perfil não alocado
TRS32	Qualificação	Manter profissionais sem formação ou sem a qualificação exigida no "Apêndice IV - Qualificação dos Profissionais" para executar os serviços contratados, durante o período de medição mensal dos Serviços.	Por ocorrência	5 pontos para cada perfil não qualificado
TRS33	Qualificação	Alocar profissional sem capacidade técnica necessária ao pleno atendimento do objeto contratado ou sem atender às qualificações exigidas no contrato, ainda que em casos de substituição temporária.	Por ocorrência	5 pontos
TRS34	Qualificação	Deixar de apresentar no prazo definido neste Termo de Referência as comprovações das qualificações técnicas dos perfis profissionais da CONTRATADA, conforme "Apêndice IV - Qualificação dos Profissionais".	Por mês incompleto de atraso	10 pontos
TRS35	Relatórios	Deixar de apresentar os relatórios consolidados para a fiscalização contratual, conforme exigências e prazos definidos no Termo de Referência da contratação.	Por dia de atraso	1 ponto
TRS36	Relatórios	Deixar de apresentar relatórios, levantamentos e inventários no prazo determinado em comum acordo.	Por ocorrência	5 pontos
TRS37	Requisição Planejada	Deixar de realizar a avaliação de impacto, criação de cronograma, monitoramento e controle do processo de mudança, ou realizá-los de forma deficiente ou incompleta, quando se tratar de Requisições Planejadas.	Por ocorrência	10 pontos
TRS38	Requisição Planejada	Deixar de comunicar a realização de Requisições Planejadas que poderão gerar indisponibilidade em sistemas ou serviços.	Por ocorrência	10 pontos

TRS39	Requisição Planejada	Deixar de executar as Requisições Planejadas no Tempo Máximo para Solução definido pela Contratante na Demanda de Serviço ou outra metodologia definida pela Contratante.	Por ocorrência	10 pontos
TRS40	Reunião	Deixar de participar de reunião solicitada e previamente agendada com a equipe de gestão de TI do CONTRATANTE, presencial ou remota.	Por ocorrência	5 pontos
TRS41	Segurança orgânica	Deixar de zelar pela segurança orgânica das instalações do contratante, fornecendo crachá ou credenciais de acesso a pessoas não autorizadas, ou ainda não verificando o correto fechamento das portas das áreas restritas.	Por ocorrência	10 pontos
TRS42	Serviços	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços solicitados.	Por ocorrência	10 pontos
TRS43	Serviços	Causar qualquer indisponibilidade dos serviços do CONTRATANTE por motivo de imperícia na execução das atividades contratuais.	Por ocorrência	10 pontos
TRS44	Serviços	Recusar-se a executar serviço relacionado ao objeto do contrato, determinado pela fiscalização, por serviço.	Por ocorrência	10 pontos
TRS45	Serviços	Interromper unilateralmente a prestação de serviços sem que haja evento de força maior que o justifique.	Por dia de interrupção	10 pontos
TRS46	Uso Indevido	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares, etc.) ou utilizar equipamento particular, salvo em situação excepcional e devidamente autorizado pelo CONTRATANTE.	Por ocorrência	5 pontos
TRS47	Zelo	Deixar de zelar pelas máquinas, equipamentos e instalações do CONTRATANTE utilizados pela CONTRATADA.	Por ocorrência	5 pontos



Documento assinado eletronicamente por **Rafael de Lima Ramos, Coordenador(a)**, em 01/09/2026, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Alysson Marques, Coordenador-Geral**, em 01/09/2026, às 11:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0811192** e o código CRC **894771A2**.

Referência: Processo nº 00100.002198/2025-02

SEI nº 0811192

LICITAÇÃO: ANEXO Nº ETP 6//2026 - APÊNDICE VI -/2026/ASSESSOR- DITEC/DITEC

Processo nº 00100.002198/2025-02

Interessado: CGISE

APÊNDICE VI - ESPECIFICAÇÕES TÉCNICAS

SOLUÇÃO DE GERENCIAMENTO DE SERVIÇOS DE TIC E PLATAFORMA DE OBSERVABILIDADE AVANÇADA COM IA PARA OPERAÇÕES DE TI (AIOPS)

1. CONTEXTUALIZAÇÃO

1.1. A solução de gerenciamento de serviços de TIC atualmente em uso no ITI é o *Open Source Ticket Request System* (OTRS) cuja é mantida pela atual equipe de operação de infraestrutura. Contudo, dada as mudanças estratégicas e operacionais, não atende por completo às áreas e atuais demandas do ITI. De forma que se faz necessária a sua substituição pela nova CONTRATAÇÃO, proibindo através desta contratação fornecimento de solução open source e soluções SaaS.

1.2. É de conhecimento de todos que as soluções de gerenciamento de TIC comercializadas possuem diferentes variáveis de licenciamento ou subscrição, que podem incluir o número de usuários ou o número de atendentes, por exemplo, dentre outras.

1.3. Cabe ressaltar que, para os itens de serviço constantes da presente contratação, está prevista uma equipe mínima que poderá sofrer alterações face à necessidade de cumprimento do nível mínimo de serviço exigido, impactando no número de atendentes, que inclusive podem aumentar apenas de forma sazonal, em períodos em que a CONTRATADA entender que o ajuste dos seus profissionais seja necessário para alcance do INS.

1.4. Somado a isso, há a complexidade das parametrizações, customizações e automações necessárias e que deverão ser implementadas pela CONTRATADA ao longo do Contrato, que requerem o total conhecimento e domínio técnico e comercial da ferramenta, além, é claro, das permissões de evolução tecnológica e alterações na solução, que podem depender do tipo de licenciamento ou da política do fabricante do software.

1.5. O modelo adotado atualmente, em que a CONTRATADA é responsável pelo fornecimento, manutenção e evolução da solução ITSM, facilita a gestão para o

ITI, não impacta nas fronteiras de responsabilidade que ocorre nos casos de múltiplos contratos e não requer a manutenção de um contrato adicional de suporte técnico e evolução somente para a solução.

1.6. Além disso, está sendo prevista nessa contratação a integração da solução de gerenciamento de TIC com o TEAMS e a criação de *chatbots* que possibilitarão que os usuários utilizem o mesmo canal para abertura e acompanhamento de chamados, otimizando o processo de demandas. Para essa condição, além do conhecimento técnico para a integração do TEAMS com a solução, também será necessário que a CONTRATADA tenha total conhecimento das especificidades dos serviços e seus respectivos INS, bem como da dinâmica das Equipes Técnicas, corroborando para a vantajosidade da manutenção do fornecimento da ferramenta pela mesma CONTRATADA dos serviços de operação da infraestrutura.

1.7. Para o correto dimensionamento da solução de gerenciamento de serviços de TIC, no que se refere à utilização pelo ITI, deverá estar compreendido o quantitativo de usuários discriminado no "Apêndice I - Infraestrutura de TIC", compreendendo servidores, terceirizados e parceiros do ITI. Cabe ressaltar que a quantidade de usuários atendentes previstas para o ITI são complementares às licenças que a CONTRATADA deverá prever para a sua equipe.

1.8. É de responsabilidade total da CONTRATADA a identificação e fornecimento do quantitativo e tipo de licenças necessários à execução dos serviços, devendo abranger todos os usuários do ITI.

2. REQUISITOS DA SOLUÇÃO DE ITSM

2.1. A solução de software de *Information Technology Service Management (ITSM)* para Gerenciamento de Serviços de TIC e Conformidade deverá estar em conformidade com pelo menos 15 (quinze) da biblioteca de boas práticas ITIL v4, com no mínimo os requisitos listados abaixo, por se tratar das práticas cuja implantação estão previstas na presente contratação.

2.2. A Solução de ITSM e CONFORMIDADE poderá ser composta por uma ou mais ferramentas, desde que totalmente integradas e compatíveis entre si, e deverão ser providenciados todos os softwares e licenças necessários à execução dos serviços e completa implantação das disciplinas ITIL. Isto significa, por exemplo, que deve ser disponibilizada pela CONTRATADA ferramenta para inventário de ativos de TIC como resultado da implantação do processo de Gerenciamento de Ativos de TI.

2.3. No que tange aos processos ITIL v4, a solução deverá permitir a implantação de todos os processos ao longo do Contrato sem necessidade de aquisição de módulos complementares.

2.4. A solução poderá ser instalada na infraestrutura de TI no ITI deverá:

- I. Os serviços cadastrados devem permitir o vínculo com ativos suportados.
- II. Os serviços cadastrados devem permitir o vínculo do Cliente demandante do serviço.
- III. Os serviços cadastrados devem permitir o vínculo com contratos.
- IV. A solução deve fornecer aplicativo móvel com suporte para sistemas operacionais android e IOS, permitindo o acompanhamento do chamados e abertura de chamados através do aplicativo móvel.
- V. O aplicativo móvel deve estar nas lojas oficiais de suporte do Sistema operacional Android Play Store e IOS App Store.

VI. VI - Ser fornecida com licenciamento perpetuo visando a continuidade do histórico do ITI.

- 2.4.1. Deve permitir a criação de um Relatório de Causa Raiz.
- 2.4.2. O relatório de Causa Raiz deve permitir o registro técnico da ocorrência.
- 2.4.3. O relatório de Causa Raiz deve permitir o registro de uma Solução de Contorno.
- 2.4.4. Deve possuir um formulário para registro de Mudanças.
- 2.4.5. A aplicação deve possuir módulo para emissão de relatórios e dashboards com indicadores triviais para a tomada de decisão da Gestão.
- 2.4.6. Deve permitir a vinculação entre indicadores e relatórios com atualização dinâmica de resultados. Os resultados devem ser exibidos em diversos níveis de detalhamento, permitindo a análise desde o desempenho global, parcial ou individual dos indicadores.
- 2.4.7. Deve possuir relatório que aponte a quantidade de chamado atendido por cada Analista.
- 2.4.8. A aplicação deve permitir, a autenticação de usuários via SSO (Single Sing On/Login único) de forma Segura.
- 2.4.9. A aplicação deve permitir a autenticação via tecnologia OAuth2.
- 2.4.10. Deve ser permitido a autenticação com uso da tecnologia OAuth2, utilizada em sistemas como o Microsoft Office365, Google, dentre outros.
- 2.4.11. Deve ser permitido aos administradores definirem domínios válidos para a autenticação via OAuth.
- 2.4.12. Deve ser bloqueado todo e qualquer acesso não configurado pelo administrador.
- 2.4.13. O sistema deve possibilitar o envio de notificações via whatsapp para usuários sobre atualizações em seus chamados.
- 2.4.14. O sistema deve possibilitar o envio de notificações via sistema Telegram para usuários sobre atualizações em seus chamados.
- 2.4.15. O sistema deve possibilitar o envio de notificações via sistema Microsoft Teams
- 2.4.16. A SOLUÇÃO deverá ser aplicação web multiusuário e multiorganização, composta por interface de página única, camada de serviço (API) e banco de dados relacional, acessível por navegador sem instalação de cliente nas estações.
- 2.4.17. A SOLUÇÃO deverá ser instalada na infraestrutura do CONTRATANTE, próprio, com operação integral em rede fechada, sem exigir saída para a internet e sem tráfego de dados de atendimento para serviços de terceiros.
- 2.4.18. A SOLUÇÃO deverá dispor de instalador completo para sistemas operacionais Windows e macOS, contemplando aplicação, tempo de execução, banco de dados e registro dos serviços em pacote único, admitida implantação assistida em Linux ou em contêineres.
- 2.4.19. A SOLUÇÃO deverá operar, em sua totalidade, incluindo banco de dados e o componente de inteligência artificial, sobre um único servidor de porte padrão, dispensando parque dedicado de servidores.
- 2.4.20. O licenciamento da SOLUÇÃO não poderá ser vinculado à quantidade de atendentes, agentes ou usuários nomeados, de modo que a ampliação da equipe de

atendimento não implique acréscimo de valor.

2.4.21. A SOLUÇÃO não poderá depender, para seu funcionamento, de licença adicional, módulo pago à parte, complemento ou serviço em nuvem de terceiros, devendo a integração com sistemas externos ser opcional e não condicionante da operação.

2.4.22. A interface da SOLUÇÃO, suas mensagens e sua documentação deverão estar integralmente em português do Brasil.

2.4.23. A SOLUÇÃO deverá oferecer filtros globais de período e de organização aplicáveis às telas de análise, alternância entre tema claro e escuro e exportação de relatórios em formato PDF.

2.4.24. As telas de operação deverão dispor de atualização automática de dados em intervalo configurável, não superior a 30 segundos no menor intervalo disponível.

2.4.25. A SOLUÇÃO deverá registrar chamados classificados, no mínimo, como incidente e como requisição de serviço, mantendo a distinção ao longo de todo o ciclo de vida e na apuração contratual.

2.4.26. A prioridade do chamado deverá ser calculada automaticamente pelo cruzamento de urgência e impacto em matriz 5x5, vedada a digitação direta do campo prioridade pelo usuário.

2.4.27. A SOLUÇÃO deverá aceitar a abertura de chamados por, no mínimo, quatro canais: console do atendente, portal de autoatendimento, mensagem de correio eletrônico e rotina programada, todos alimentando a mesma fila e sujeitos às mesmas regras.

2.4.28. A SOLUÇÃO deverá permitir o anexo de imagens, vídeos e documentos na abertura e durante o atendimento, com controle de acesso ao download.

2.4.29. A SOLUÇÃO deverá permitir o agendamento de data e hora desejadas para o início do atendimento no momento da abertura.

2.4.30. O ciclo de vida do chamado deverá contemplar, no mínimo, os estados novo, em atendimento, aguardando atendimento, pendente, encaminhado a fornecedor, solucionado e fechado, com transições controladas pela própria SOLUÇÃO, vedado o salto de etapas.

2.4.31. A SOLUÇÃO deverá dispor de mecanismo de captura que impeça o atendimento simultâneo do mesmo chamado por mais de um atendente, com possibilidade de devolução do chamado à fila.

2.4.32. O chamado deverá manter registro segregado de acompanhamentos, tarefas, solução, anexos e histórico, sendo o histórico imutável e integralmente auditável.

2.4.33. A SOLUÇÃO deverá oferecer modelos de acompanhamento que padronizem as respostas ao solicitante.

2.4.34. A SOLUÇÃO deverá permitir o escalonamento do chamado entre níveis de atendimento, no mínimo primeiro, segundo e terceiro níveis, especialista e coordenação, com motivo obrigatório, troca de grupo responsável e registro em linha do tempo.

2.4.35. O "pendenciamento" de chamado deverá exigir justificativa, permitir lembrete de retomada e suspender a contagem do prazo de nível de serviço enquanto perdurar a pendência.

2.4.36. A SOLUÇÃO deverá permitir o encaminhamento do chamado a

fornecedor externo, com registro do protocolo do terceiro e status próprio visível na fila.

2.4.37. O encerramento técnico do chamado deverá exigir o registro da solução, com classificação do tipo de solução e evidências, facultada a publicação do conteúdo na base de conhecimento.

2.4.38. Após a solução, a SOLUÇÃO deverá abrir prazo para avaliação e reabertura pelo solicitante, com fechamento automático ao término do prazo, tudo registrado na linha do tempo.

2.4.39. A SOLUÇÃO deverá medir separadamente o tempo ativo e o tempo suspenso de cada chamado, refletindo a segregação nos indicadores e na apuração contratual.

2.4.40. A SOLUÇÃO deverá controlar, no mínimo, dois prazos por chamado: tempo para primeiro atendimento e tempo para resolução.

2.4.41. A SOLUÇÃO deverá diferenciar acordos de nível de serviço firmados com o contratante, acordos internos entre equipes e acordos de apoio firmados com fornecedores.

2.4.42. As metas de prazo deverão ser parametrizáveis por prioridade e por item do catálogo de serviços, admitida meta específica por organização contratante, com precedência sobre o padrão do catálogo.

2.4.43. A SOLUÇÃO deverá suportar regime de cobertura ininterrupta e regime de horário útil, este último apoiado em calendário com faixas de expediente por dia da semana, fuso horário e cadastro de feriados.

2.4.44. A contagem do prazo deverá ser suspensa enquanto o chamado depender de terceiro, retomando a contagem na volta ao atendimento.

2.4.45. A SOLUÇÃO deverá sinalizar o risco de descumprimento do prazo em faixas objetivas e utilizar o mesmo critério de cálculo em painéis de operação, painéis gerenciais e apuração contratual.

2.4.46. Ao esgotar-se o prazo de resolução, a SOLUÇÃO deverá elevar automaticamente o chamado ao nível de atendimento seguinte, notificar os canais configurados e registrar o evento de forma durável.

2.4.47. A SOLUÇÃO deverá dispor de motor de regras próprio, configurável por administrador sem desenvolvimento, com condições sobre título, descrição, organização, origem, requerente, localidade e setor, admitidos operadores de conteúdo, igualdade, prefixo e expressão, combináveis por conjunção e disjunção.

2.4.48. As regras deverão poder definir categoria, prioridade, tipo, grupo técnico, nível de atendimento, acordo de nível de serviço e responsável pelo chamado.

2.4.49. A SOLUÇÃO deverá permitir ordenar a avaliação das regras, interromper o processamento a partir de determinada regra e restringir o escopo de aplicação por unidade organizacional.

2.4.50. A SOLUÇÃO deverá dispor de simulador que permita testar as regras configuradas sem criar chamado real.

2.4.51. A SOLUÇÃO deverá permitir a abertura automática de chamados em periodicidade programada, com frequência diária, semanal ou mensal, hora definida e exibição da próxima execução.

2.4.52. A SOLUÇÃO deverá abrir chamados automaticamente a partir de caixa de correio eletrônico monitorada e converter em acompanhamento a resposta que

contenha o número do chamado.

2.4.53. A SOLUÇÃO deverá notificar as movimentações do chamado por correio eletrônico, por ferramenta corporativa de mensageria e por aviso interno, com roteamento por nível de atendimento.

2.4.54. A SOLUÇÃO deverá encerrar automaticamente o chamado solucionado cujo prazo de manifestação do solicitante tenha decorrido, registrando o fechamento.

2.4.55. A SOLUÇÃO deverá dispor de gestão de problemas, com registro de causa raiz, erro conhecido e solução de contorno, controle de estados até a eliminação definitiva e vínculo bidirecional com os incidentes de origem.

2.4.56. A SOLUÇÃO deverá dispor de gestão de mudanças, com classificação em normal, padrão e emergencial, planos de implantação e de reversão obrigatórios e vínculo aos itens de configuração afetados.

2.4.57. As mudanças deverão submeter-se a comitê de aprovação, com quórum mínimo parametrizável, sem o qual a mudança não avança.

2.4.58. A SOLUÇÃO deverá dispor de gestão de liberação, com versão, janela e lista de verificação, admitindo na composição do pacote apenas mudanças previamente aprovadas pelo comitê.

2.4.59. A SOLUÇÃO deverá registrar a implantação por ambiente, no mínimo desenvolvimento, homologação, pré-produção e produção, com status e reversão registrados por ambiente.

2.4.60. A SOLUÇÃO deverá apurar a disponibilidade por serviço e por item de configuração, calculando percentual de disponibilidade, número de falhas, tempo indisponível, tempo médio entre falhas e tempo médio de recuperação, com registro das janelas de indisponibilidade e emissão de relatório do período.

2.4.61. A SOLUÇÃO deverá dispor de catálogo de serviços organizado por grupos, contendo por oferta a categoria, o tipo, o acordo de nível de serviço aplicável e a elegibilidade de nível de atendimento, com roteamento automático da solicitação.

2.4.62. A SOLUÇÃO deverá permitir a criação de modelos de chamado com campos pré-preenchidos, obrigatórios e ocultos, aplicáveis por precedência entre categoria, perfil, unidade e padrão geral.

2.4.63. A SOLUÇÃO deverá registrar oportunidades de melhoria contínua, com origem rastreada, prioridade, responsável, benefício esperado quantificado e fluxo de status até a conclusão.

2.4.64. A SOLUÇÃO deverá manter cadastro de fornecedores e de contratos de apoio, com vigência e valor mensal, e controle de licenças de software vinculadas aos ativos.

2.4.65. A SOLUÇÃO deverá registrar riscos do serviço, avaliados por probabilidade e impacto, com tratamento e acompanhamento.

2.4.66. A SOLUÇÃO deverá manter inventário de itens de configuração com tipo, fabricante, número de série, número de Patrimônio, localidade e contrato.

2.4.66.1. A SOLUÇÃO deve permitir atrelar o contrato ao item/ativo registrado, permitir gerar QR CODE com identificação para cada item registrado de forma individual, permitindo controle e abertura de chamado através do QR CODE do dispositivo.

2.4.66.2. Deve ser permitido impressão da tag individual ou em massa, para ser

inserido no ativo físico.

2.4.67. Os itens de configuração deverão ter ciclo de vida controlado, contemplando ao menos os estados novo, em uso, em estoque, em reparo e baixado.

2.4.68. A SOLUÇÃO deverá registrar relacionamentos entre itens de configuração, contemplando ao menos as relações de dependência, conexão, execução, hospedagem e composição, para avaliação de impacto.

2.4.69. Cada item de configuração deverá possuir linha do tempo com histórico de eventos, incluindo as indisponibilidades registradas.

2.4.70. A SOLUÇÃO deverá vincular itens de configuração a chamados, problemas e mudanças.

2.4.71. A SOLUÇÃO deverá dispor de base de conhecimento com fluxo de aprovação em três estados, organização por categoria, busca, contador de visualizações e marcação de conteúdo público para o portal.

2.4.72. A SOLUÇÃO deverá permitir a publicação de artigo na base de conhecimento diretamente a partir do registro de solução do chamado.

2.4.73. A SOLUÇÃO deverá registrar a aprovação, pelo CONTRATANTE, dos procedimentos operacionais publicados, servindo o registro como evidência de homologação.

2.4.74. A SOLUÇÃO deverá dispor de painel de monitoração contínua que exiba apenas os chamados que demandam ação, segregados em recortes de aguardando captura, prazo vencido, prazo em iminência de vencimento, prazo em alerta e prazo suspenso.

2.4.75. O painel de monitoração deverá dispor de modo de exibição em tela cheia para projeção na central, atualização automática e busca por número, organização ou responsável.

2.4.76. O painel de monitoração deverá dispor de alerta sonoro para novos eventos críticos, destinado à operação em regime de plantão.

2.4.77. A SOLUÇÃO deverá dispor de quadro visual de fluxo de trabalho, organizado por estado, com limite de trabalho em andamento configurável por coluna, sinalização de excedente e movimentação do cartão por arrastar e soltar.

2.4.78. A SOLUÇÃO deverá calcular métricas de fluxo, contemplando ao menos tempo total de atendimento, tempo sob responsabilidade da equipe e eficiência de fluxo, apresentando média e mediana.

2.4.79. A fila de chamados deverá dispor de painel de acompanhamento calculado sobre todo o conjunto filtrado e de filtros por estado, tipo, prioridade, organização, responsável e período.

2.4.80. A SOLUÇÃO deverá dispor de painel executivo consolidado, contendo ao menos volume, chamados em aberto, tempo médio de primeiro atendimento, tempo médio de resolução, cumprimento de prazo, satisfação e tendência de abertos contra resolvidos.

2.4.81. A SOLUÇÃO deverá dispor de painel operacional com indicadores-chave, feed de alertas com registro de escalonamento, visão consolidada por organização e controle do prazo de resolução.

2.4.82. Os indicadores apresentados nos painéis deverão ser navegáveis, permitindo abrir a relação dos chamados que compõem cada número.

2.4.83. A SOLUÇÃO deverá apresentar o desempenho do atendimento por

prioridade, por nível de equipe, por atendente e por satisfação do solicitante, com evolução mensal contra a meta.

2.4.84. A SOLUÇÃO deverá apresentar a distribuição da demanda no tempo, contemplando o envelhecimento dos chamados em aberto por faixa de espera, o volume resolvido por semana e a concentração por dia da semana e hora do dia.

2.4.85. A SOLUÇÃO deverá permitir a análise individual do atendente, com tempos de atendimento, proporção entre tempo ativo e suspenso e distribuição por prioridade, admitida a comparação entre atendentes com correção estatística por volume de amostra.

2.4.86. A SOLUÇÃO deverá apresentar, por organização contratante, o volume e a qualidade do atendimento confrontados com o custo apurado e a receita do contrato, com classificação automática da saúde contratual.

2.4.87. A SOLUÇÃO deverá apurar o custo do atendimento a partir de custo cadastrado por nível de atendimento e de custo individual por atendente, prevalecendo o custo individual quando existente.

2.4.88. A SOLUÇÃO deverá permitir a parametrização, por administrador e sem desenvolvimento, das faixas que classificam a carga de trabalho do atendente.

2.4.89. A SOLUÇÃO deverá oferecer análise de correlação entre as séries históricas da operação e representação gráfica dos relacionamentos entre chamados, organizações, atendentes, ativos e serviços.

2.4.90. A SOLUÇÃO deverá emitir relatórios em formato PDF, em modelo institucional, respeitando os filtros de período e organização aplicados na tela.

2.4.91. A SOLUÇÃO deverá calcular e apresentar, no mínimo, os indicadores de chamados em aberto, tempo médio de primeiro atendimento, tempo médio de resolução, cumprimento de prazo, satisfação, envelhecimento, volume resolvido, tempo total, tempo sob responsabilidade da equipe, eficiência de fluxo, disponibilidade e tempo suspenso.

2.4.92. A SOLUÇÃO deverá dispor de instrumento de medição de resultado nativo, com indicadores configuráveis por contrato, contemplando ao menos cumprimento do prazo de solução, cumprimento do prazo de resposta, chamados em aberto, satisfação e tempo médio de resolução.

2.4.93. Cada indicador do instrumento de medição deverá admitir meta e peso, devendo a soma dos pesos totalizar cem por cento.

2.4.94. A SOLUÇÃO deverá calcular o desconto por descumprimento a partir de faixas parametrizáveis por indicador, apresentando a glosa ponderada, o valor do desconto e o valor líquido a pagar na competência.

2.4.95. A apuração deverá ser calculada diretamente sobre os chamados efetivamente registrados na competência, vedada a alimentação manual dos resultados.

2.4.96. A SOLUÇÃO deverá admitir modelo alternativo de apuração por pontuação de ocorrências de inadimplemento, com conversão em percentual de desconto, teto configurável e fatores de aplicação progressiva em período de estabilização.

2.4.97. A medição da competência deverá ser exportável em formato PDF, apta a instruir o processo de pagamento.

2.4.98. A SOLUÇÃO deverá registrar Ordens de Serviço por contrato, com controle de status até o faturamento.

- 2.4.99. A SOLUÇÃO deverá suportar a medição por resultado e a fiscalização contratual nos termos da Lei nº 14.133/2021 e da IN SGD/ME nº 94/2022, registrando a execução e mantendo trilha para prestação de contas.
- 2.4.100. A SOLUÇÃO deverá dispor de perfis de uso distintos, contemplando ao menos administração, atendimento pleno, atendimento com escopo reduzido, consulta gerencial, gestão pelo contratante e solicitante.
- 2.4.101. Além do perfil de uso, a SOLUÇÃO deverá permitir a composição de perfis de acesso por página, devendo a restrição ser aplicada também na camada de serviço, de modo que o acesso negado não possa ser obtido por endereço direto.
- 2.4.102. A SOLUÇÃO deverá restringir a visibilidade dos dados por organização e por unidade organizacional, admitindo visão consolidada apenas aos perfis autorizados.
- 2.4.103. A SOLUÇÃO deverá suportar autenticação em dois fatores, com códigos de recuperação.
- 2.4.104. A SOLUÇÃO deverá exigir a troca de senha no primeiro acesso do usuário.
- 2.4.105. As credenciais de integração com sistemas externos deverão ser armazenadas de forma cifrada.
- 2.4.106. A SOLUÇÃO deverá manter trilha de auditoria das ações administrativas, classificada por sensibilidade e consultável por período, usuário e tipo de ação.
- 2.4.107. O histórico de cada chamado deverá ser imutável, complementando a trilha de auditoria da plataforma.
- 2.4.108. Em ambiente que atenda a mais de uma organização, a SOLUÇÃO deverá isolar os dados de cada uma em base própria.
- 2.4.109. A SOLUÇÃO deverá dispor de fluxo de solicitação de acesso pelo próprio interessado, submetido a aprovação do administrador, com vinculação à organização correta e senha temporária de exibição única.
- 2.4.110. A SOLUÇÃO deverá permitir a marcação do chamado que contenha dados pessoais, com registro da base legal e da finalidade do tratamento.
- 2.4.111. A SOLUÇÃO deverá registrar e controlar as solicitações de titular de dados previstas no art. 18 da Lei nº 13.709/2018, com controle do prazo legal de resposta.
- 2.4.112. A SOLUÇÃO deverá executar a anonimização de chamados encerrados, preservando o registro operacional necessário à estatística contratual.
- 2.4.113. A SOLUÇÃO deverá dispor de política de retenção e identificar os registros elegíveis a expurgo.
- 2.4.114. O tratamento dos dados deverá ocorrer exclusivamente na infraestrutura do CONTRATANTE, sem transferência de conteúdo de atendimento a terceiros, inclusive quanto a recursos de inteligência artificial.
- 2.4.115. A SOLUÇÃO deverá oferecer assistente de consulta em linguagem natural, em português, disponível ao atendente em qualquer tela do console e ao solicitante no portal.
- 2.4.116. O processamento do assistente deverá ocorrer na infraestrutura do CONTRATANTE, sem envio de conteúdo de chamados a serviços externos e sem cobrança por consulta.
- 2.4.117. O assistente deverá permanecer operante em ambiente sem saída para a internet.

- 2.4.118. A SOLUÇÃO deverá dispor de portal de autoatendimento apartado do console de atendimento, no qual o solicitante abra, acompanhe, avalie e reabra seus chamados.
- 2.4.119. O portal deverá permitir a abertura de chamado por texto livre e por seleção de oferta do catálogo de serviços, com anexo de arquivos.
- 2.4.120. O portal deverá restringir a visibilidade dos chamados ao próprio solicitante, admitida visão de todos os chamados da organização ao perfil de gestão do CONTRATANTE.
- 2.4.121. O portal deverá disponibilizar consulta à base de conhecimento pública e emissão, pelo próprio solicitante, de relatório de seus chamados no período.
- 2.4.122. O portal deverá permitir a avaliação do atendimento em escala numérica e a reabertura do chamado dentro do prazo definido, alimentando o indicador de satisfação do contrato.
- 2.4.123. A SOLUÇÃO deverá importar o histórico de chamados de ferramenta anterior a partir de arquivos em formato CSV, XLS ou XLSX, com mapeamento de colunas conferível e pré-visualização antes da gravação.
- 2.4.124. A importação deverá preservar a data original de abertura e o número de origem de cada chamado.
- 2.4.125. A importação deverá normalizar estado, prioridade e tipo, tornando o histórico pesquisável e integrado aos indicadores desde a entrada em produção.
- 2.4.126. Os dados deverão residir em banco sob guarda do CONTRATANTE, com exportação em formato estruturado, vedada qualquer forma de retenção que dificulte a substituição da SOLUÇÃO.
- 2.4.127. A SOLUÇÃO deverá dispor de painel de conformidade que relacione as práticas de gestão de serviços adotadas e as normas de governança de referência, apontando, para cada item, a tela que comprova o atendimento.
- 2.4.128. O painel de conformidade deverá contemplar, no mínimo, as referências ITIL 4, ISO/IEC 20000, COBIT, práticas de fluxo enxuto, gestão de conhecimento centrada em solução, ISO 9001 e ISO/IEC 27001 e 27701, além das normas de contratação pública aplicáveis.
- 2.4.129. A CONTRATADA deverá entregar documentação de uso completa, em português, cobrindo todos os módulos da SOLUÇÃO, do primeiro acesso à apuração contratual, com indicação do caminho de menu e do passo a passo de cada tarefa.
- 2.4.130. A CONTRATADA deverá capacitar as equipes de atendimento de primeiro a terceiro nível e disponibilizar o portal aos solicitantes na entrada em produção, com operação assistida no período inicial.
- 2.4.131. A CONTRATADA deverá realizar prova de conceito na infraestrutura do CONTRATANTE, por período determinado, com dados reais de contrato ou área piloto, previamente à aceitação definitiva.
- 2.4.132. A documentação deverá contemplar as rotinas operacionais recomendadas em periodicidade diária, semanal e mensal, incluindo o fechamento da competência para fins de medição.
- 2.4.133. A sustentação da SOLUÇÃO, compreendendo suporte, correção de defeitos e disponibilização de novas versões, deverá ser de responsabilidade da CONTRATADA, sem transferência a comunidade de usuários ou a terceiros.
- 2.4.134. A SOLUÇÃO deve disponibilizar painéis de monitoramento de status de chamado para monitoria e acompanhamento, com indicadores e alertas, permitindo

interação direto pela pagina de monitoria.

3. PLATAFORMA DE MONITORAMENTO AVANÇADO COM IA PARA OPERAÇÕES DE TI - DISPOSIÇÕES GERAIS

3.1. A solução deverá ser implantada em ambiente de nuvem pública, privada ou híbrida, sob responsabilidade da CONTRATANTE, devendo:

- I. Suportar arquitetura distribuída e escalável horizontalmente (scale-out), com balanceamento automático de carga entre componentes;
- II. Garantir isolamento lógico e segurança dos dados, independentemente do modelo de implantação;
- III. Permitir operação em ambientes híbridos, com coleta e processamento de dados provenientes de múltiplas regiões e provedores;
- IV. Suportar alta disponibilidade nativa, com mecanismos de failover automático entre instâncias;
- V. Garantir continuidade operacional mesmo em caso de falha de componentes individuais da plataforma.
- VI. Admitir a implantação em rede fechada, sem saída para a internet, hipótese em que a coleta e a execução remota se darão por componente instalado no ambiente da CONTRATANTE.

3.2. Escalabilidade e Performance

- I. Suportar crescimento progressivo do volume de dados (métricas, logs, eventos e traces) sem degradação perceptível de desempenho;
- II. Permitir expansão de capacidade de processamento e armazenamento sem necessidade de interrupção do serviço;
- III. Operar com baixa latência na ingestão e análise de dados, permitindo processamento em tempo real ou próximo ao tempo real;
- IV. Garantir desempenho consistente mesmo sob cenários de alta volumetria de eventos e métricas.

3.3. Licenciamento e Componentes

- I. Todos os módulos, componentes, conectores, agentes, APIs e funcionalidades necessárias ao pleno atendimento dos requisitos desta especificação deverão estar contemplados na proposta técnico-financeira
- II. Não será admitida a necessidade de aquisição adicional de módulos, plugins ou extensões para atendimento dos requisitos técnicos descritos;
- III. A solução deverá possuir modelo de licenciamento unificado, evitando fragmentação entre componentes;
- IV. Eventuais limitações técnicas decorrentes de licenciamento deverão ser explicitadas na proposta.

3.4. Controle de Acesso e Perfis

- I. Prover acesso simultâneo a, no mínimo:
 - 100 (cem) usuários finais;
 - 20 (vinte) usuários com perfil de operação, administração ou resolução;
 - 05 (cinco) usuários com perfil analítico avançado.

- II. Permitir licenciamento não nominal, possibilitando o remanejamento dinâmico de usuários;
- III. Implementar controle de acesso baseado em papéis (RBAC), permitindo granularidade na definição de permissões;
- IV. Permitir segregação de funções entre usuários, garantindo aderência a boas práticas de governança;
- V. Registrar logs de auditoria detalhados de acesso, incluindo:
 - a) identificação do usuário;
 - b) data e hora;
 - c) ações realizadas

3.5. **Interface e Experiência de Uso**

- I. Possuir interface 100% web, acessível via navegador, sem necessidade de instalação de componentes locais;
- II. Ser compatível com os principais navegadores de mercado;
- III. Permitir operação responsiva, com adaptação a diferentes resoluções de tela;
- IV. Disponibilizar interface no idioma português brasileiro;
- V. Permitir personalização de dashboards, painéis e visualizações por perfil de usuário;
- VI. Permitir navegação entre diferentes níveis de informação (visão executiva → técnica → detalhada), com suporte a drill-down.

3.6. **Segurança da Informação**

- I. Garantir criptografia de dados em trânsito e em repouso;
- II. Permitir integração com mecanismos de autenticação corporativa (ex: LDAP, Active Directory, SSO);
- III. Suportar autenticação multifator (MFA);
- IV. Garantir proteção de credenciais utilizadas na coleta de dados (ex: discovery, integrações);
- V. Manter trilha de auditoria completa das ações realizadas na plataforma;
- VI. Permitir configuração de políticas de retenção de dados conforme requisitos da CONTRATANTE.

3.7. **Integração e Interoperabilidade**

- I. Disponibilizar APIs abertas para integração com sistemas externos;
- II. Permitir ingestão de dados provenientes de múltiplas fontes (on-premise e cloud);
- III. Suportar integração com ferramentas de monitoração, automação e segurança;
- IV. Permitir exportação de dados para ferramentas analíticas externas;
- V. Garantir consistência e integridade dos dados integrados.

3.8. **Observabilidade e Inteligência Operacional**

- I. Operar como plataforma unificada de observabilidade, integrando métricas, eventos, logs e rastreamento de transações;
- II. Permitir correlação automática entre dados de diferentes camadas (infraestrutura, aplicação e serviço);
- III. Suportar análise em tempo real e histórica;
- IV. Integrar-se com mecanismos de inteligência artificial para análise preditiva, detecção de anomalias e automação de resposta;
- V. Garantir atualização contínua das informações monitoradas

3.9. **Ingestão e Deduplicação de Alertas**

- a) A solução deverá receber alertas provenientes de múltiplas fontes de monitoramento por meio de webhooks HTTP, suportando, no mínimo, os formatos: Grafana Alert Manager, Prometheus Alert Manager, PagerDuty Events API e Zabbix Webhooks.
- b) A solução deverá suportar ingestão de pacotes enriquecidos contendo alertas correlacionados, inventário de hosts afetados, topologia de serviços e histórico de alterações recentes.
- c) A solução deverá implementar mecanismo de deduplicação de alertas com mesma origem e identificador, recebidos dentro de uma janela temporal configurável, de modo a evitar abertura duplicada de incidentes.
- d) A solução deverá suportar ingestão do tipo pull-based (polling) a partir de plataformas externas de AIOps por meio de adaptadores configuráveis.
- e) A solução deverá criar incidentes automaticamente a partir dos alertas recebidos, atribuindo severidade, hosts afetados e contexto extraído do payload do alerta.
- f) A solução deverá manter separados, em registros distintos, a caracterização do evento e a decisão de acionamento correspondente, de modo que cada decisão possa ser auditada independentemente do evento que a originou.
- g) A solução não deverá basear a decisão de acionamento exclusivamente em rótulo de severidade ou em nome de grupo atribuídos pela fonte, devendo considerar, no mínimo: desvio em relação à linha de base observada, especificidade do alvo, correlação com sinal interno e evidência de falha do controle.
- h) A solução não deverá realizar supressão silenciosa de eventos, devendo todo evento suprimido ser registrado com o critério que fundamentou a supressão.
- i) A solução deverá apurar e disponibilizar as taxas de supressão e de acionamento por fonte e por período, para verificação da efetividade da triagem.

3.10. **Gestão de Incidentes**

- a) Cada incidente deverá possuir ciclo de vida definido contemplando, no mínimo, os estados: detecção, investigação, aguardando aprovação, investigado, resolvido e encerrado, com possibilidade de transição para estado de escalção a qualquer momento.
- b) A solução deverá classificar incidentes por severidade em pelo menos cinco níveis: Crítico, Alto, Médio, Baixo e Informativo.

- c) A solução deverá atribuir número sequencial por organização para referência humana dos incidentes.
- d) A solução deverá permitir listagem de incidentes com filtros por status, severidade, fonte, período, hosts afetados e equipe responsável.
- e) A solução deverá exibir linha do tempo (timeline) completa de cada incidente, incluindo alertas recebidos, ações executadas, resultados das verificações, decisões do agente de IA e interações humanas.
- f) A solução deverá suportar investigação automática de incidentes com base em critérios de severidade configuráveis pelo administrador.
- g) A solução deverá distinguir o estado 'investigado' (agente concluiu a análise) do estado 'resolvido' (problema confirmado como solucionado), admitindo que a transição entre eles seja realizada pelo operador humano ou de forma automática, a partir do evento de mudança de status emitido pela solução de ITSM integrada.

3.11. **Investigação Autônoma por Agente de Inteligência Artificial**

- a) A solução deverá executar ciclo iterativo de raciocínio, ação e observação de forma autônoma para investigar incidentes, selecionando e invocando capacidades apropriadas com base no contexto do incidente.
- b) A solução deverá suportar a execução de ações sobre a infraestrutura, incluindo: execução de comandos em hosts afetados, consulta de métricas em fontes de dados, consulta de logs, verificação de conectividade e abertura de chamados na solução de gestão de serviços (ITSM) por webhook autenticado por chave de API, com correlação por identificador externo.
- c) A solução deverá respeitar níveis de risco configuráveis para execução de ações, de modo que: ações de baixo risco sejam executadas automaticamente; ações de risco médio sejam executadas com registro detalhado; ações de alto risco e críticas exijam aprovação humana prévia.
- d) A solução deverá implementar critérios de parada automáticos para o ciclo de investigação, incluindo: número máximo de iterações configurável, ausência de progresso detectada em iterações consecutivas, atingimento de limiar de confiança e timeout global configurável.
- e) A solução deverá registrar cada decisão, raciocínio, ação executada e resultado observado pelo agente, garantindo auditabilidade e reprodutibilidade das investigações.
- f) A solução deverá suportar, no mínimo, três modos de operação: autônomo (agente investiga e resolve sem intervenção humana, exceto ações destrutivas); assistido (agente investiga e sugere ações, operador decide); e manual (agente atua como assistente via chat, operador conduz).
- g) A solução deverá permitir a definição do grau de autonomia por classe de ação e por ambiente, de modo que uma mesma ação possa ser executada automaticamente em um ambiente e estar sujeita a aprovação humana em outro, sem necessidade de desenvolvimento, devendo toda ação automática registrar o procedimento de reversão aplicável.

3.12. **Orquestração Multi-Agente**

- a) A solução deverá suportar planejamento de investigações complexas como grafo acíclico dirigido (DAG), permitindo que passos independentes sejam executados em paralelo.

- b) O planejador de execução paralela deverá ser acionado por meio de modelo de linguagem, gerando automaticamente o plano com as dependências entre as etapas de investigação.
- c) A solução deverá suportar hooks configuráveis em pontos críticos do fluxo de execução, incluindo antes do uso de ferramenta, após geração do plano e ao acionar subagentes.

3.13. **Conjunto de Capacidades Nativas**

3.13.1. A solução deverá prover conjunto de capacidades nativas que o agente de IA poderá acionar durante investigações, incluindo no mínimo:

- Execução de comandos em hosts remotos via SSH e em ambientes isolados (sandbox);
- Consulta de métricas, dashboards e regras de alerta em plataformas de monitoramento (ex.: Grafana, Prometheus);
- Consulta a fontes de dados heterogêneas (ex.: ClickHouse, PostgreSQL, Elasticsearch) por meio de SQL ou linguagens de consulta nativas;
- Abertura de chamados, registro de acompanhamentos e encerramento na solução de ITSM integrada;
- Envio de notificações por múltiplos canais (ex.: Slack, Microsoft Teams, Telegram, e-mail);
- Verificação de conectividade de serviços por meio de probes HTTP/HTTPS, TCP, DNS, SSL/TLS, ICMP e SMTP;
- Geração de documentos técnicos a partir de modelos (templates) pré-definidos;
- Análise de métricas históricas e calibração automática de limiares de alerta;
- Consulta a inventário e topologia de configuração de serviços.

3.13.2. A execução de comandos em hosts remotos deverá implementar pipeline de segurança multicamadas, contemplando: decomposição de comandos compostos, validação de redirecionamentos para caminhos protegidos, classificação de risco por padrões de comandos, restrições por ambiente (desenvolvimento, homologação, produção) e classificação contextual por modelo de linguagem para comandos ambíguos.

3.13.3. A solução deverá permitir habilitação e desabilitação granular de cada capacidade por organização/tenant.

3.13.4. A solução deverá registrar métricas de uso por capacidade: total de execuções, taxa de sucesso, latência média e custo estimado em tokens.

3.14. **Interface Conversacional com Agente de IA**

- a) A solução deverá oferecer interface de chat com o agente de IA em dois modos: (a) vinculado a um incidente específico, com acesso a toda a linha do tempo, evidências, hosts afetados e aos dados do chamado correlacionado na solução de ITSM, recebidos por evento de integração; e (b) assistente geral de infraestrutura com acesso às capacidades e integrações configuradas.
- b) O chat deverá suportar transmissão de respostas em tempo real (streaming), exibindo ao operador o raciocínio do agente, o início e o resultado de cada ação executada, solicitações de aprovação humana e mensagens de erro.

- c) O chat deverá suportar retomada de sessão após desconexão, reconstruindo o contexto a partir do histórico de mensagens armazenado.
- d) A solução deverá aplicar controles de uso configuráveis por organização, incluindo: limite de mensagens por minuto, limite de execuções de capacidades por minuto, número máximo de conversas simultâneas e orçamento de tokens por conversa e por turno.
- e) O estilo de saída do agente deverá ser configurável em ao menos três níveis hierárquicos — organização, usuário e conversa —suportando modos como conciso, normal, detalhado e estruturado.

3.15. **Automações Programadas**

- a) A solução deverá suportar criação de rotinas automatizadas com frequência configurável, incluindo: execução manual, horária, diária, em dias úteis, semanal, mensal e cron customizado.
- b) As rotinas deverão ser definidas por meio de descrição em linguagem natural, com suporte a referências inline a capacidades e agentes disponíveis.
- c) A solução deverá permitir ativação, desativação e pausa de rotinas, registrando histórico de execuções com data, hora, duração, status (sucesso ou falha) e sumário do resultado.
- d) As rotinas deverão suportar execução via orquestração multi-agente paralela e memória episódica para aprendizado com execuções anteriores.

3.16. **Geração Automatizada de Documentos**

- a) A solução deverá suportar geração de documentos técnicos a partir de modelos (templates) com resolução automática de variáveis a partir de fontes como: dados do incidente, métricas coletadas, dados do chamado correlacionado na solução de ITSM (número, título, organização, prioridade, status e nível de atendimento) e consultas a fontes de dados externas.
- b) A solução deverá disponibilizar, no mínimo, os seguintes tipos de documento nativos: análise de causa raiz (RCA), relatório de incidente, relatório de desempenho de aplicações, relatório de calibração de alertas e planejamento de capacidade.
- c) Os documentos gerados deverão possuir ciclo de vida com os estados: rascunho, revisão, aprovado e publicado, com suporte a versionamento e histórico de alterações.
- d) A solução deverá suportar exportação dos documentos no formato PDF.
- e) A solução deverá suportar agendamento de geração periódica de documentos com entrega automática por e-mail e por canais de mensageria configurados.

3.17. **Dashboard Operacional**

- a) A solução deverá disponibilizar painel central de operações com atualização em tempo real, exibindo: total de incidentes ativos e tendência, tempo médio de resolução (MTTR), taxa de automação (percentual de incidentes resolvidos sem intervenção humana) e aprovações pendentes.
- b) O painel deverá exibir tabela de incidentes com filtros por severidade, status, equipe e período.

- c) O painel deverá exibir feed de atividade ao vivo com eventos do agente, das integrações e das ações dos operadores.
- d) O painel deverá exibir status de saúde das integrações configuradas.

3.18. **Aprovações e Escalações**

- a) A solução deverá suportar fluxo de aprovação humana para ações de risco elevado, com notificação ao aprovador pelo canal configurado (ex.: Slack, Teams, e-mail).
- b) A solução deverá suportar regras de escalação configuráveis, incluindo: timeout de aprovação, escalação automática e cadeia de escalação (operador, líder, gestor).
- c) A solução deverá cancelar automaticamente operações cujo timeout de aprovação expire, adotando comportamento fail-closed (operação não realizada em caso de ausência de resposta).

3.19. **Integrações com Sistemas Externos**

3.19.1. A solução deverá suportar integração nativa com, no mínimo, as seguintes categorias de sistemas:

- Gestão de Serviços de TI (ITSM): integração por interface de programação de aplicações (API) e por webhook autenticado por chave, com abertura e encerramento de chamados e correlação bidirecional por identificador externo;
- Monitoramento: Grafana, Prometheus, Zabbix;
- Fontes de dados: ClickHouse, PostgreSQL, Elasticsearch;
- Notificação: Slack, Microsoft Teams, Telegram, e-mail (SMTP);
- Execução remota: SSH (hosts Linux/Unix) e Kubernetes.

3.19.2. Todas as integrações deverão implementar mecanismos de retry com backoff exponencial, circuit breaker por provedor, timeout configurável, rate limiting e verificação periódica de saúde (health check).

3.19.3. A solução deverá suportar troca de integrações sem necessidade de reinicialização do serviço (hot-swap).

3.19.4. A solução deverá suportar modo de execução remota para ambientes sem acesso direto de rede, por meio de agente instalado no ambiente do cliente que se comunica com a plataforma via protocolo seguro.

3.19.5. A solução deverá admitir coletores distribuídos por região, cada um com identificação única, sem exposição de portas de rede e com criptografia ponta a ponta entre o coletor e a plataforma.

3.20. **Integração com Gestão de Serviços de TI (ITSM)**

- a) A solução deverá abrir chamados na solução de ITSM automaticamente após a conclusão de investigações, com base em severidade mínima configurável, convertendo a severidade do incidente em urgência e impacto, de modo que a prioridade do chamado seja derivada da matriz da própria solução de ITSM.
- b) A solução deverá acompanhar o status dos chamados abertos e encerrar incidentes automaticamente quando o chamado correspondente for fechado na solução de ITSM, admitido o acompanhamento por evento emitido pela solução de ITSM a cada mudança de status do chamado.

- c) A solução deverá manter rastreabilidade bidirecional entre incidentes e chamados da solução de ITSM, por identificador externo persistido no próprio chamado.

3.21. **Base de Conhecimento**

- a) A solução deverá suportar cadastro e gestão de entradas de conhecimento, com busca por similaridade semântica (busca vetorial) para enriquecer o contexto do agente durante investigações.
- b) O agente deverá consultar a base de conhecimento durante investigações, alcançando os artigos, erros conhecidos e soluções de contorno registrados na solução de ITSM, e incorporar as soluções conhecidas ao raciocínio e às recomendações geradas.

3.22. **Execução em Ambiente Isolado**

- a) A solução deverá disponibilizar ambiente de execução isolado (sandbox) onde o agente possa executar comandos sem acesso ao ambiente de produção, com restrições de sistema de arquivos, rede, privilégios e recursos computacionais.
- b) A solução deverá disponibilizar terminal interativo no ambiente isolado, acessível via interface web em tempo real.
- c) A solução deverá suportar provisionamento e desprovisionamento dinâmico dos ambientes isolados com escalonamento automático baseado na demanda.

3.23. **Orquestração de Modelos de Linguagem**

- a) A solução deverá registrar, de forma auditável, todas as chamadas realizadas a sistemas externos, incluindo: método, URL, corpo da requisição e resposta (sanitizados), status HTTP, decomposição de latência e contagem de tentativas.
- b) A solução deverá registrar cada iteração do ciclo de investigação do agente, incluindo: número da iteração, fase, raciocínio, ação executada, parâmetros utilizados, resultado observado e duração.
- c) O roteamento dos modelos deverá ser configurável por tipo de atividade, permitindo definir qual modelo será utilizado para cada contexto (investigação de incidentes, geração de documentos, chat, sumarização, entre outros).
- d) O módulo de orquestração de LLMs deverá permitir a definição de orçamento mensal por organização e por finalidade, com alerta em percentual configurável e comportamento definido para o esgotamento do orçamento, contemplando, no mínimo, as opções de bloqueio, degradação para modelo de menor custo ou continuidade com registro, conforme configuração da CONTRATANTE.

3.24. **Observabilidade da Plataforma**

- a) A solução deverá registrar, de forma auditável, todas as chamadas realizadas a sistemas externos, incluindo: método, URL, corpo da requisição e resposta (sanitizados), status HTTP, decomposição de latência e contagem de tentativas.
- b) A solução deverá registrar cada iteração do ciclo de investigação do agente,

incluindo: número da iteração, fase, raciocínio, ação executada, parâmetros utilizados, resultado observado e duração.

- c) A solução deverá registrar cada chamada realizada a modelos de linguagem, incluindo: provedor, modelo, tokens de entrada e saída, custo estimado, latência e motivo de encerramento.
- d) Todos os eventos de observabilidade deverão ser disponibilizados em tempo real na interface da plataforma, permitindo filtro por investigação.
- e) A solução deverá suportar rastreamento distribuído aderente ao padrão OpenTelemetry, permitindo visibilidade end-to-end desde a ingestão do alerta até a resolução do incidente.
- f) O registro de observabilidade deverá permitir reconstituir integralmente a decisão automatizada a partir dos dados persistidos, incluindo: entrada, raciocínio, ação executada, parâmetros utilizados, resultado observado e modelo utilizado, de modo que a fiscalização possa auditar a decisão sem depender de nova execução.

3.25. **Identidade e Controle de Acesso**

- a) A solução deverá implementar controle de acesso baseado em papéis (RBAC), com isolamento completo de dados entre organizações (multi-tenant).
- b) A solução deverá suportar, no mínimo, os seguintes papéis: administrador, líder técnico (SRE Lead), operador, visualizador e aprovador.
- c) A solução deverá suportar os seguintes métodos de autenticação: usuário e senha com token JWT, Single Sign-On (SSO) via OIDC (ex.: Google Workspace, Azure AD, Okta) e SAML 2.0 para integração corporativa.
- d) A solução deverá suportar autenticação multifator (MFA) com TOTP e WebAuthn/FIDO2, configurável como obrigatório por organização.
- e) A solução deverá suportar autenticação por chaves de API para integrações máquina-a-máquina.
- f) A solução deverá implementar isolamento de dados no nível de banco de dados (Row Level Security) para garantir que cada organização acesse exclusivamente seus próprios dados.

3.26. **Requisitos Não Funcionais**

- a) Desempenho: o tempo entre o recebimento do alerta e o início da primeira ação de investigação deverá ser inferior a 30 (trinta) segundos.
- b) Disponibilidade: a solução deverá garantir disponibilidade mínima de 99,5% (noventa e nove vírgula cinco por cento) ao longo do período contratual.
- c) Segurança: credenciais armazenadas deverão ser criptografadas com algoritmos de padrão industrial (ex.: AES-256); chaves de API deverão ser armazenadas somente como hash irreversível; toda operação sensível deverá gerar registro de auditoria imutável; containers de execução deverão operar sem privilégios elevados.
- d) Escalabilidade: a arquitetura deverá suportar expansão horizontal de componentes sem interrupção do serviço.
- e) Dados: todas as informações armazenadas são de propriedade exclusiva da CONTRATANTE e deverão ser disponibilizadas em sua integralidade por, no mínimo, 120 (cento e vinte) dias após o encerramento do contrato.

- f) Atualizações: a versão ofertada deverá ser a mais recente e estável disponível, e o fornecedor deverá prover atualizações corretivas e evolutivas durante toda a vigência contratual.
- g) Sincronização de horário: todos os componentes da solução deverão sincronizar o horário automaticamente com a Hora Legal Brasileira (Observatório Nacional).

3.27. **Módulo de Discovery / Inventário de Ativos de TI**

- a) A solução deverá ser capaz de realizar a descoberta de uma ampla variedade de dispositivos, incluindo licenças de software, servidores físicos e virtuais, storages, dispositivos de rede, buckets de armazenamento em nuvem, containers (Kubernetes, OpenShift, Rancher, Docker, AWS ECS, Azure AKS, Oracle OKE, entre outros) e demais ativos existentes no parque tecnológico, suportando relacionamentos muitos-para-muitos ou pai-filho entre os itens descobertos, incluindo nuvens públicas (AWS, Azure, Huawei, Oracle, Google, VMware, entre outras), ambientes virtualizados e infraestruturas distribuídas.
- b) A solução deverá manter as funcionalidades essenciais de gestão de configuração (CMDB) na solução de ITSM, contemplando criação, leitura, atualização e desativação de itens de configuração (ICs), bem como as funcionalidades essenciais de gestão de ativos de TI, admitida a carga do inventário descoberto por importação a partir da ferramenta de descoberta.
- c) A solução deverá entender e interpretar os diferentes modelos de serviço em nuvem, como IaaS (Infrastructure as a Service) e PaaS (Platform as a Service), com suporte à descoberta de recursos em várias regiões, proporcionando visão consolidada de ambientes distribuídos geograficamente.
- d) A solução deverá realizar a descoberta utilizando método sem agente instalado nos alvos (agentless), podendo complementar com método baseado em agente para descoberta em tempo real, desde que não afete o desempenho dos alvos.
- e) A solução deverá notificar os responsáveis imediatamente sobre a descoberta de dispositivos não autorizados e, ao identificá-los, ser capaz de bloqueá-los ou isolá-los mediante integração com ferramentas de segurança.
- f) A solução deverá manter agenda de execução da descoberta em intervalos regulares, garantindo a integridade dos dados do CMDB, com possibilidade de definir e personalizar o escopo da descoberta (segmentos de rede, tipos de IC e de ativo a incluir ou excluir).
- g) A solução deverá suportar uso de protocolos de descoberta como, no mínimo: SNMP, WMI e SSH, garantindo que a descoberta seja realizada de forma segura, com proteção de credenciais e adesão às melhores práticas de segurança.
- h) A solução deverá apresentar mapa de relacionamentos e dependências em visualização gráfica ou diagramas interativos, atualizado em tempo real, com suporte a tipos de relacionamento como “é parte de”, “é conectado a”, “depende de” e “é usado por”, independente da camada representada (serviço, aplicação, infraestrutura).
- i) A solução deverá criar automaticamente versões do mapa de relacionamentos e dependências, mantendo histórico de versões anteriores,

com rastreabilidade de alterações ao longo do tempo.

- j) A solução deverá realizar auditorias automáticas para verificação da existência e conformidade dos ICs no parque tecnológico, identificando não conformidades e sugerindo correções.
- k) A integração do módulo de Discovery com a solução de ITSM deverá ocorrer por interface de programação de aplicações (API), contemplando a importação do inventário descoberto e a atualização dos itens de configuração no CMDB.
- l) A solução deverá realizar a descoberta e a classificação automática de ativos nas camadas física e lógica, construindo topologia e mapa de dependências que contemplem, no mínimo: equipamentos de armazenamento, empilhamento de comutadores, telefonia sobre IP e demais elementos de rede, bem como componentes de nuvem pública, apresentados no mesmo grafo de dependências que os ativos locais.
- m) O componente instalado nos ativos monitorados deverá ser único para as funções de monitoração e de inventário e não poderá exigir a exposição de porta de serviço em escuta no ativo, de modo que a monitoração não amplie a superfície de ataque do parque tecnológico.
- n) A solução deverá reconciliar os registros provenientes de fontes distintas de descoberta e inventário, deduplicando por precedência configurável entre fontes, de modo que o mesmo ativo descoberto por mais de um método resulte em um único item de configuração, com registro da fonte que prevaleceu em cada atributo.

3.28. **Módulo de AIOps - Requisitos Complementares**

- a) A solução de AIOps deverá possuir capacidades avançadas de inteligência artificial para identificar automaticamente a causa raiz dos eventos, sem necessidade de configurações manuais prévias, aprendendo continuamente com cada evento para melhorar a precisão das suas previsões e recomendações.
- b) A solução deverá exibir visualmente a topologia de serviços com base nas dependências entre componentes de infraestrutura (ICs), mostrando os impactos de um chamado em um serviço mapeado pela ferramenta de descoberta, e integrar-se à solução de ITSM para automação do fluxo de resolução de incidentes, desde a abertura até o encerramento do chamado.
- c) A solução deverá ter capacidade de integração com sistemas de monitoramento de nuvem, para captura de eventos das soluções CloudWatch da AWS, Azure Monitor, Google Cloud Monitoring e OCI Monitoring da Oracle, fornecendo visão unificada de problemas ocorridos em nuvem e no on-premise.
- d) A solução deverá ser capaz de rastrear o impacto na disponibilidade de um item de configuração com base em dados do mapa de relacionamento, incidentes e problemas causados por alterações anteriores, identificando a causa raiz como erro conhecido registrado na solução de ITSM e aplicando a solução de contorno nele mapeada.
- e) A solução deverá ser capaz de configurar limites de performance para itens de configuração com flexibilidade para diferentes cenários e períodos (sazonalidade), identificando redução de qualidade/performance do serviço em virtude de tempo de resposta elevado, mesmo que não afete a disponibilidade contratada.

- f) A solução deverá possuir recursos de inteligência artificial para propor possíveis diagnósticos ou resoluções para chamados, a partir da análise dos dados do chamado e do conhecimento acumulado na solução de ITSM (base de conhecimento, chamados anteriores, mudanças, itens de configuração e eventos), cabendo ao motor de regras da solução de ITSM o direcionamento do chamado no fluxo de trabalho definido.
- g) A solução deverá estar preparada para ativação de recursos de IA Generativa, oferecendo interface conversacional em linguagem natural para usuários finais e equipes de TI, gerando respostas automatizadas e contextualizadas para incidentes, solicitações de serviço e perguntas frequentes.
- h) A solução deverá ser flexível e conectável a LLMs de mercado (como OpenAI, entre outros) via API, possibilitando personalização e alternância entre modelos.
- i) Toda a arquitetura, inclusive o AIOps, deverá ser instalada de modo que todos os seus dados sejam processados e armazenados dentro da infraestrutura da CONTRATANTE, com modelo de licenciamento unificado para toda a plataforma.

3.29. **Módulo de Gestão de Eventos**

- a) A solução deverá ser capaz de detectar anomalias e picos de eventos, agrupando e relacionando eventos e alertas, e abrir chamados automaticamente na solução de ITSM a partir de um evento, iniciando o fluxo de gestão de incidentes conforme critérios definidos pela CONTRATANTE e o conteúdo do evento, com deduplicação por identificador externo e admitida a reclassificação do chamado para requisição de serviço, problema ou mudança na própria solução de ITSM.
- b) A solução deverá executar ações corretivas automatizadas para os eventos identificados e ser capaz de avaliar a série histórica do item de configuração e projetar horizonte de evolução, identificando proativamente risco de descumprimento da disponibilidade acordada e recomendando a ação de ajuste correspondente, com registro da projeção e do seu fundamento, observado o grau de autonomia definido pela CONTRATANTE, nos termos do item 3.11, registrando a ação executada no chamado correspondente na solução de ITSM, que dará origem ao registro de mudança quando aplicável.
- c) A solução deverá ter capacidade de integração com ferramentas essenciais de monitoramento e operações como Zabbix, Prometheus e VMware Aria Operations para sincronização de eventos e topologia (ICs), além de integração com sistemas de monitoramento de nuvem (CloudWatch, Azure Monitor, Google Cloud Monitoring e OCI Monitoring da Oracle).
- d) A solução deverá ser capaz de receber evento de normalização do objeto do incidente e realizar automaticamente os procedimentos de encerramento adequados conforme regra de negócio definida pela CONTRATANTE, bem como medir a disponibilidade efetiva de um IC/Serviço e informar ao módulo de gestão de níveis de serviço da solução de ITSM para aferição do indicador.

3.30. **Módulo de Monitoramento de Performance de Aplicações (APM)**

- a) A solução deverá permitir o monitoramento de transações de aplicações em tempo real, contemplando, no mínimo: tempo de resposta, volume de transações (throughput) e taxa de erro, possibilitando análise detalhada do

comportamento das aplicações.

- b) A solução deverá realizar rastreamento distribuído (distributed tracing) de transações ponta a ponta, identificando automaticamente o caminho completo de uma requisição entre múltiplos serviços, APIs e componentes, e identificar gargalos de desempenho ao longo da execução, indicando o ponto exato de degradação.
- c) A solução deverá identificar automaticamente as dependências entre componentes de aplicação e entre aplicações e infraestrutura, permitindo visualização da topologia lógica e técnica das aplicações monitoradas, com correlação entre dados de aplicação, infraestrutura, eventos e métricas em visão unificada. A topologia de aplicação deverá ser reconciliada com o inventário e o mapa de dependências produzidos pelo módulo de descoberta (item 3.27), de modo que aplicação e infraestrutura sejam representadas no mesmo grafo de dependências.
- d) A solução deverá definir automaticamente um baseline de comportamento das aplicações com base em dados históricos, detectando anomalias de performance por desvios do comportamento esperado e gerando alertas automaticamente quando houver degradação significativa, mesmo sem violação de thresholds previamente definidos.
- e) A solução deverá operar em ambientes distribuídos e baseados em microsserviços, incluindo integração com plataformas de orquestração de containers (ex.: Kubernetes), e permitir armazenamento de dados históricos de performance para análise retrospectiva, identificação de tendências e suporte à tomada de decisão para otimização de desempenho.

3.31. **Módulo de Disponibilidade e Capacidade**

- a) A solução deverá medir a disponibilidade efetiva de um IC/Serviço, considerando a agenda de disponibilidade contratada (regime de produção) e agrupamentos de serviço, apresentando a disponibilidade por meio de diversas métricas como MTBF, MTRS, número de serviços impactados, tempo total de indisponibilidade por período e tempo mínimo entre falhas.
- b) A solução deverá calcular disponibilidade end-to-end do serviço sob a perspectiva do usuário final, considerando toda a cadeia de dependências, identificar proativamente ameaças à meta de disponibilidade e avaliar a série histórica do item de configuração e projetar horizonte de evolução, recomendando (via AIOps) a ação de ajuste necessária para prevenir o descumprimento da disponibilidade ou da capacidade acordada, com registro da projeção e do seu fundamento, observado o grau de autonomia definido pela CONTRATANTE, nos termos do item 3.11.
- c) A solução deverá permitir o registro da capacidade total e utilizada dos recursos de TI (CPU, memória, armazenamento em disco, taxas de transferência de rede, latência de resposta, entre outros), fornecendo visão consolidada de capacidade por Segmento Tecnológico e Tipo de Ativo, com armazenamento de dados históricos para análise retrospectiva e tendências.
- d) A solução deverá suportar a criação de Acordo de Nível de Serviço (ANS) padrão aplicável a todos os serviços e fluxos, registrando os períodos regulares de aferição dos níveis de serviço acordados, com possibilidade de fracionamento sob demanda, e notificando os responsáveis sobre proximidade de quebra e violação efetiva de ANS por correio eletrônico e por ferramenta corporativa de mensageria, com escalonamento automático do chamado.

4. PLATAFORMA DE ORQUESTRAÇÃO DE CONHECIMENTO COM LLMS EM LOW-CODE E LLMOPS

4.1. Disposições Gerais

- a) A plataforma deverá ser disponibilizada em modalidade de software como serviço (SaaS) ou implantada em infraestrutura on-premises ou nuvem privada da CONTRATANTE, conforme definição no ato convocatório.
- b) A plataforma deverá suportar múltiplos usuários com papéis diferenciados, contemplando: desenvolvedores de soluções de IA, usuários finais de agentes e administradores da plataforma.
- c) A interface da plataforma deverá estar disponível no idioma português brasileiro e ser acessível por navegador web sem instalação de cliente dedicado.
- d) Todos os módulos e integrações necessários para atendimento desta especificação deverão estar incluídos na proposta, não sendo admitida cobrança adicional por componentes não declarados.

4.2. Orquestração de Prompts e Operações de LLMs (LLMOps)

- a) A plataforma deverá oferecer interface visual intuitiva para orquestração de prompts e gerenciamento de fluxos de trabalho com modelos de linguagem, sem necessidade de programação extensiva.
- b) A plataforma deverá ser agnóstica em relação ao provedor de modelos de linguagem, suportando integração com, no mínimo, os seguintes provedores: OpenAI (família GPT), Anthropic (família Claude) e Google (família Gemini), permitindo inclusão de novos provedores sem alteração estrutural da plataforma.
- c) A plataforma deverá oferecer ferramentas integradas de LLMOps para gerenciamento e otimização de modelos de linguagem, abrangendo desde a experimentação inicial até a implantação em ambiente de produção.
- d) A plataforma deverá disponibilizar interface de gerenciamento para rastreamento de dados, custos e consumo dos modelos de linguagem, com recursos para melhoria contínua de desempenho.
- e) A plataforma deverá suportar ferramentas para engenharia de prompts, permitindo criação, teste, versionamento e reutilização de prompts de forma estruturada.
- f) A plataforma deverá suportar múltiplos estilos de saída dos agentes, configuráveis por contexto de uso.

4.3. Fluxos de Trabalho em Low-Code

- a) A plataforma deverá disponibilizar ambiente de desenvolvimento de soluções de IA com abordagem low-code, permitindo que equipes com pouca ou nenhuma experiência em programação criem e gerenciem aplicações de IA.
- b) A plataforma deverá suportar criação e modificação de pipelines de automação por meio de interface visual intuitiva, permitindo prototipagem rápida e iteração de soluções.
- c) A plataforma deverá permitir a criação de componentes reutilizáveis entre diferentes fluxos de trabalho.
- d) A plataforma deverá disponibilizar painel de controle específico para

consulta, edição, execução e monitoramento dos fluxos criados.

- e) A plataforma deverá suportar a programação de execução dos fluxos ao menos das seguintes formas: agendada (schedule), manual pelo usuário e automática por eventos ou ações de outros sistemas.
- f) A plataforma deverá disponibilizar dashboard com métricas e gráficos do histórico de execuções dos fluxos de trabalho.
- g) A plataforma deverá prover ambientes segregados para desenvolvimento, teste e produção.

4.4. Motores de Recuperação com Auxílio de Contexto (RAG) e Ingestão de Conhecimento

- a) A plataforma deverá disponibilizar motores de Recuperação com Auxílio (RAG — Retrieval-Augmented Generation) de alta qualidade, permitindo combinar dados contextuais com modelos de linguagem para respostas mais precisas e contextualmente relevantes.
- b) A plataforma deverá suportar implementação de fluxo RAG completo, incluindo: ingestão de dados, pré-processamento, fragmentação (chunking), geração de embeddings, armazenamento em banco de dados vetorial e geração de resposta pelo LLM a partir de prompts do usuário.
- c) A plataforma deverá suportar conectores de ingestão de dados que facilitem a acessibilidade, atualização e usabilidade dos dados nas bases de conhecimento.
- d) A plataforma deverá permitir particionamento, limpeza e preparação de dados antes da análise principal.
- e) A plataforma deverá suportar decomposição de textos longos em segmentos menores e consistentes, com configuração de estratégias de fragmentação.
- f) A plataforma deverá converter dados textuais em vetores de tamanho fixo (embeddings) e armazená-los de forma otimizada para buscas de alta velocidade por similaridade semântica.
- g) A plataforma deverá suportar decomposição de textos em tokens e integração nativa com modelos de linguagem próprios e externos.

4.5. Processamento e Particionamento de Documentos

- a) A plataforma deverá suportar processamento e reconhecimento de ao menos os seguintes formatos de arquivo: texto simples (TXT), planilhas (XLS, XLSX, CSV), JSON, PDF, HTML, Markdown, PowerPoint, e-mails e EPUB.
- b) A plataforma deverá realizar detecção automática do tipo de arquivo para roteamento ao processador apropriado.
- c) A plataforma deverá permitir a configuração de opções específicas de particionamento por tipo de documento.
- d) A plataforma deverá permitir a extração de metadados relevantes e a estruturação do conteúdo de documentos.
- e) A plataforma deverá suportar reconhecimento óptico de caracteres (OCR) para processamento de documentos digitalizados, com suporte a múltiplos idiomas.
- f) A plataforma deverá disponibilizar APIs para particionamento de documentos, permitindo integração com sistemas existentes e automação de fluxos de trabalho.

- g) A plataforma deverá permitir atualização das bases de dados de conhecimento em períodos pré-definidos e customização dos modelos de IA com novas informações a qualquer momento.

4.6. Agentes de Inteligência Artificial Personalizáveis

- a) A plataforma deverá oferecer estrutura flexível para criação de agentes de IA personalizáveis, com configuração de comportamento, personalidade e capacidades conforme as necessidades específicas do caso de uso.
- b) A plataforma deverá permitir a utilização dos agentes criados em diversas aplicações, incluindo atendimento ao cidadão, assistentes virtuais especializados e automação de processos, com integração aos sistemas corporativos.
- c) A plataforma deverá suportar flexibilidade para customizar as ações executadas pelos agentes de IA.
- d) A plataforma deverá disponibilizar ferramentas de publicação dos agentes e aplicações diretamente na plataforma.

4.7. APIs e Integrações

- a) A plataforma deverá disponibilizar APIs RESTful para integração com sistemas existentes, permitindo que a lógica de negócios seja desacoplada dos prompts e do motor de IA, e consumir a solução de ITSM por webhook autenticado por chave de API.
- b) A plataforma deverá suportar integração com a solução de gestão de serviços adotada na organização, por interface de programação de aplicações e por eventos nos dois sentidos, permitindo gestão centralizada e eficiente.
- c) A plataforma deverá suportar integração com bancos de dados, webservices, arquivos CSV e correio eletrônico, com envio por SMTP e recebimento por IMAP.
- d) A plataforma deverá suportar tecnologias padrão de integração, incluindo SOAP, REST, JSON e WSDL.
- e) A plataforma deverá permitir integração de dados de múltiplas fontes para alimentar o motor de IA.
- f) A plataforma deverá suportar autenticação do tipo SSO (Single Sign-On), com integração a diretórios corporativos como Active Directory e LDAP.

4.8. Gestão de Modelos e Base de Conhecimento

- a) A plataforma deverá fornecer base de conhecimento centralizada para armazenamento, gerenciamento e acesso a informações relacionadas aos modelos de IA, prompts e fluxos de trabalho, facilitando reutilização e melhoria contínua.
- b) A plataforma deverá oferecer sistema de gestão de modelos com suporte a documentação, rastreamento de alterações e auditoria completa dos projetos de IA.
- c) A plataforma deverá disponibilizar ferramentas de anotação (annotation) para refinamento de modelos com base em feedbacks contínuos dos usuários.
- d) A plataforma deverá permitir personalização e adaptação dos modelos de

linguagem para atendimento às necessidades específicas da organização, incluindo a capacidade de ajuste fino (fine-tuning) de modelos.

4.9. Monitoramento, Avaliação e Extensibilidade

- a) A plataforma deverá incluir ferramentas de monitoramento de desempenho dos modelos e aplicações em produção, permitindo ajustes em tempo real.
- b) A plataforma deverá disponibilizar extensões personalizáveis para adaptação a cenários e setores específicos.
- c) A plataforma deverá suportar a análise automática de dados e fornecimento de insights relevantes a partir dos fluxos executados.
- d) A plataforma deverá possibilitar armazenamento de logs por período mínimo de 30 (trinta) dias, com possibilidade de ampliação desse prazo.
- e) A plataforma deverá permitir a realização de backups periódicos das configurações, modelos e bases de conhecimento.

4.10. Análise de Dados e Aprendizado de Máquina

- a) A plataforma deverá possuir funcionalidades de análise de dados (Data Analytics) com suporte a criação de dashboards dinâmicos por arrastar e soltar (drag & drop).
- b) A plataforma deverá permitir definição de indicadores-chave de desempenho (KPIs), projeção de tendências em métricas e detecção de anomalias.
- c) A plataforma deverá suportar análise e modelagem de séries temporais e modelagem de classificação e regressão.
- d) A plataforma deverá possibilitar análises históricas e aplicação de filtros e agrupamentos nos dashboards.
- e) A plataforma deverá suportar otimização automática de hiperparâmetros dos modelos de aprendizado de máquina.
- f) A plataforma deverá suportar processamento e análise de dados de diferentes modalidades, incluindo texto e áudio.
- g) A plataforma deverá permitir integração com ferramentas de análise exploratória de dados (EDA).
- h) A plataforma deverá permitir a formulação de consultas analíticas em linguagem natural sobre as bases de dados conectadas, traduzindo-as para linguagem de consulta estruturada e apresentando ao usuário a consulta gerada antes da execução.
- i) A plataforma deverá validar sintaticamente toda consulta gerada antes da execução, com bloqueio de comandos de definição e de manipulação de dados, de leitura de arquivo do sistema, de agendamento e de execução dinâmica, e com aplicação automática de limite de linhas e de tempo máximo de execução.
- j) A plataforma deverá conectar-se às fontes de dados exclusivamente por credencial sem privilégio de escrita, verificando essa condição no cadastro da fonte e recusando credencial com privilégio administrativo.
- k) A plataforma deverá permitir o cruzamento de dados de fontes distintas sem replicação nem persistência intermediária dos dados consultados, com limite de recursos por sessão.
- l) A plataforma deverá manter registro auditável das consultas realizadas, com

identificação do usuário, fonte consultada, consulta executada e custo apurado, exportável para instrução de processo.

- m) A plataforma deverá disponibilizar representação geográfica do território brasileiro por unidade federativa e por região, aplicável às visualizações de dados.

4.11. Segurança e Governança

- a) A plataforma deverá implementar criptografia avançada para dados em repouso e em trânsito, garantindo a proteção das informações sensíveis da organização.
- b) A plataforma deverá disponibilizar governança centralizada para gerenciamento de acesso, rastreabilidade e controle sobre os dados e as operações dos modelos de IA em ambiente único.
- c) A plataforma deverá garantir conformidade com a Lei Geral de Proteção de Dados (LGPD), incluindo políticas de privacidade e controle de consentimento.
- d) A plataforma deverá implementar protocolos de segurança de acesso suportando padrões como HTTPS, TLS 1.3, autenticação multifator (MFA) e criptografia AES-256.
- e) A plataforma deverá suportar gerenciamento de identidade e acesso com autenticação forte, múltiplos níveis de permissão e integração com sistemas de diretório existentes (ex.: Active Directory, LDAP).
- f) A plataforma deverá garantir que o acesso às informações dos sistemas da CONTRATANTE seja realizado somente por usuários com os devidos privilégios de visualização e/ou extração dos dados.
- g) A plataforma deverá tratar como dado, e não como instrução, todo conteúdo proveniente de fonte externa incorporado ao contexto do modelo, com mecanismo de detecção e bloqueio de tentativas de subversão de instruções e registro do evento de bloqueio.

4.12. Escalabilidade e Infraestrutura

- a) A plataforma deverá suportar autoescalabilidade baseada em desempenho e demanda, sem intervenção manual, com provisionamento e desprovisionamento dinâmico de recursos.
- b) A plataforma deverá suportar balanceamento de carga para distribuição eficiente do tráfego e otimização de recursos.
- c) A plataforma deverá garantir disponibilidade por meio de replicação de dados e configuração de failover automático.
- d) A plataforma deverá ser compatível com múltiplos provedores de processamento e modelos em nuvem.
- e) A plataforma deverá suportar escalabilidade eficiente para lidar com cargas de trabalho variáveis, garantindo alto desempenho dos modelos de linguagem.

4.13. Requisitos Não Funcionais

- a) Propriedade dos Dados: todas as informações armazenadas são de propriedade exclusiva da CONTRATANTE e deverão ser disponibilizadas em sua integralidade por, no mínimo, 120 (cento e vinte) dias após o

encerramento contratual.

- b) Compatibilidade: a plataforma deverá ser compatível com as duas últimas versões principais dos principais navegadores web modernos (Google Chrome, Mozilla Firefox, Microsoft Edge, Safari).
- c) Atualizações: a versão ofertada deverá ser a mais recente e estável disponível, com fornecimento de atualizações corretivas e evolutivas durante toda a vigência contratual.
- d) Sincronização de horário: todos os componentes da solução deverão sincronizar o horário automaticamente com a Hora Legal Brasileira (Observatório Nacional).
- e) Custos: todos os custos necessários para a viabilização do projeto, incluindo deslocamentos, hospedagens e alimentação, deverão estar previstos na proposta, não sendo admitidas cobranças extras não declaradas.

5. PLATAFORMA DE SEGURANÇA E GOVERNANÇA DA INFORMAÇÃO

5.1. Diretrizes Gerais

5.1.1. O monitoramento dos ativos de segurança do ambiente da CONTRATANTE deverá ser realizado através de ferramenta (hardware e/ou software) que coletará as informações necessárias via agente ou sem agente para o monitoramento de segurança (SOC), em plataforma que unifique as informações, para permitir avaliação da postura de segurança da organização.

5.1.2. Os serviços descritos neste termo de referência, serão realizados totalmente baseado nas ferramentas de segurança que serão entregues nesta contratação, com processos e pessoas para operacionalizar;

5.1.3. As ferramentas que deverão ser entregues durante os serviços, estão descritas com seus requisitos técnicos de atendimento para o ambiente da CONTRATANTE.

5.1.4. Todo o processo de serviços descritos neste edital, será realizado conforme requisitos descritos das ferramentas de segurança da informação.

5.1.5. O acesso a solução de monitoramento deverá ser realizado apenas pela equipe de segurança da CONTRATANTE e a equipe de serviço de SOC da CONTRATADA;

5.1.6. Deverão ser realizadas reuniões trimestrais gerenciais para avaliação e acompanhamento dos serviços contratados;

5.1.7. A CONTRATA deve fornecer acesso a ferramenta de resultados e status de segurança para monitoramento de incidentes, controles de SLA e avaliações da prestação do serviço, com visão do ambiente de segurança da informação em um único ponto de análise.

5.1.8. A CONTRATADA deverá monitorar alertas gerados pelas soluções de Segurança, envolvendo atividades como por exemplo:

I - Monitoramento de Potenciais Ataques Cibernéticos e Hacktivismo

II - Capacidade de coleta e análise de dados de fontes distintas, incluindo redes sociais, fóruns, aplicativos de mensageria e a Deep/Dark Web.

III - Identificação de ameaças cibernéticas e atividades de hacktivismo.

IV - Notificações sobre Vulnerabilidades

V - Monitoramento constante de feeds de vulnerabilidades e malware.

VI - Emissão de alertas sobre novas vulnerabilidades que possam afetar a segurança do ambiente.

5.2. **Governança e Consultoria de Segurança**

5.2.1. Criação de Políticas de Segurança da Informação: Desenvolvimento de políticas e procedimentos alinhados às melhores práticas do mercado e frameworks de segurança da informação.

5.2.2. Recomendações Estratégicas: Suporte consultivo contínuo para a equipe de infraestrutura e gestão, com recomendações para aumentar a segurança do ambiente e otimizar a arquitetura existente.

5.3. **Análise de Eventos de Segurança**

5.3.1. Deve possuir console web para acesso ao dashboard de gerenciamento através de navegadores web padrão.

5.3.2. A interface web deve ser responsiva e compatível com dispositivos móveis (tablets e smartphones).

5.3.3. A interface deve permitir personalização de temas e layouts conforme preferências do usuário.

5.3.4. A ferramenta deve permitir criação de dashboards personalizados com widgets configuráveis.

5.3.5. A solução deve oferecer visualizações em tempo real de dados de log e eventos de segurança.

5.3.6. A ferramenta deve suportar diferentes tipos de gráficos: barras, linhas, pizza, histogramas, mapas de calor e métricas.

5.3.7. A solução deve permitir drill-down em visualizações para análise detalhada de dados.

5.3.8. A ferramenta deve oferecer dashboards pré-configurados para casos de uso comuns de segurança.

5.3.9. A ferramenta deve implementar controle de acesso baseado em funções (RBAC) com granularidade de permissões.

5.3.10. A solução deve suportar autenticação via Active Directory/LDAP.

5.3.11. A ferramenta deve suportar autenticação multifator (MFA) para acesso administrativo.

5.3.12. A solução deve permitir coleta de dados via API REST e webhooks.

5.3.13. A solução deve suportar enriquecimento de dados com informações de contexto (geolocalização, threat intelligence).

5.3.14. A ferramenta deve implementar motor de busca full-text com indexação automática de campos.

5.3.15. A solução deve suportar busca em tempo real e histórica com performance otimizada.

5.3.16. A ferramenta deve implementar correlação de eventos baseada em regras configuráveis.

- 5.3.17. A solução deve suportar análise estatística e agregações de dados.
- 5.3.18. A ferramenta deve permitir análise de tendências e padrões temporais.
- 5.3.19. A solução deve implementar detecção de anomalias baseada em machine learning.
- 5.3.20. A solução deve suportar alertas em tempo real e baseados em agregações históricas.
- 5.3.21. A solução deve permitir integração com sistemas de ticketing.
- 5.3.22. A ferramenta deve suportar notificações via webhook para integração com sistemas externos.
- 5.3.23. A ferramenta deve implementar políticas de retenção configuráveis por tipo de dado.
- 5.3.24. A ferramenta deve permitir exportação de dados em formatos padrão (JSON, CSV).
- 5.3.25. A solução deve implementar autenticação de API via tokens de acesso.
- 5.3.26. A ferramenta deve implementar rate limiting para proteção da API.
- 5.3.27. A solução deve suportar integração com plataformas de threat intelligence.
- 5.3.28. A ferramenta deve permitir integração com ferramentas de SOAR (Security Orchestration).
- 5.3.29. A solução deve suportar integração com sistemas de monitoramento (Nagios, Zabbix).
- 5.3.30. A ferramenta deve permitir integração com plataformas de nuvem (AWS, Azure, GCP).
- 5.3.31. A ferramenta deve implementar criptografia em trânsito (TLS 1.2+) para todas as comunicações.
- 5.3.32. A solução deve suportar criptografia em repouso para dados sensíveis.
- 5.3.33. A ferramenta deve implementar logs de auditoria para todas as ações administrativas.
- 5.3.34. A solução deve suportar segregação de dados por tenant em ambientes multi-tenant. A solução deve suportar retenção de dados conforme regulamentações específicas.
- 5.3.35. A ferramenta deve implementar controles de acesso para atendimento a LGPD/GDPR.
- 5.3.36. A ferramenta deve fornecer métricas de performance e saúde do sistema.
- 5.3.37. A solução deve implementar alertas para problemas de infraestrutura.
- 5.3.38. A ferramenta deve suportar monitoramento de uso de recursos (CPU, memória, disco).
- 5.3.39. A ferramenta deve permitir gerenciamento centralizado de configurações.
- 5.3.40. A solução deve suportar deployment automatizado de configurações.
- 5.3.41. A ferramenta deve implementar versionamento de configurações.
- 5.3.42. A solução deve ser compatível com sistemas operacionais Linux (Ubuntu, CentOS, RHEL).

- 5.3.43. A ferramenta deve suportar deployment em containers (Docker, Kubernetes).
- 5.3.44. A solução deve ser compatível com ambientes on-premissess.
- 5.3.45. A ferramenta deve especificar requisitos mínimos de hardware para diferentes volumes de dados.
- 5.3.46. A solução deve fornecer calculadora de dimensionamento baseada em volume de logs.
- 5.3.47. A ferramenta deve especificar todas as dependências de software necessárias.
- 5.3.48. A solução deve fornecer documentação técnica completa em português.
- 5.3.49. A solução deve suportar atualizações automáticas com rollback em caso de problemas.

5.4. **ANÁLISE E DETECÇÃO DE AMEAÇAS**

- 5.4.1. Deve possuir console web para acesso a dashboard de gerenciamento com interface intuitiva e responsiva.
- 5.4.2. A interface web deve ser flexível e permitir mineração, análise e visualização de dados de eventos e alertas de segurança.
- 5.4.3. O dashboard deve permitir navegação através de diferentes tipos de dados coletados pelos agentes de monitoramento.
- 5.4.4. Deve fornecer visualização de alertas de segurança gerados pelo servidor entral em tempo real.
- 5.4.5. Deve fornecer dashboards pré-configurados para conformidade regulatória.
- 5.4.6. Deve incluir interface para navegação no framework MITRE ATT&CK e alertas relacionados.
- 5.4.7. Deve implementar controle de acesso baseado em funções (RBAC) com granularidade de permissões.
- 5.4.8. Deve incluir monitoramento do Registry do Windows com detecção de alterações maliciosas.
- 5.4.9. Deve implementar detecção de malware através de monitoramento de integridade de arquivos e regras de detecção de ameaças.
- 5.4.10. Deve suportar listas CDB (Custom Database) e integração com feeds de threat intelligence.
- 5.4.11. Deve implementar integração nativa para análise de arquivos suspeitos.
- 5.4.12. Deve fornecer scripts de resposta ativa pré-configurados para cenários comuns.
- 5.4.13. Deve permitir criação e implementação de scripts de resposta ativa customizados.
- 5.4.14. Deve permitir configuração flexível do módulo SCA com políticas personalizáveis.
- 5.4.15. Deve fornecer políticas SCA pré-configuradas para diferentes sistemas operacionais e aplicações.
- 5.4.16. Deve implementar detecção automática de vulnerabilidades em sistemas e aplicações monitorados.

5.4.17. Deve implementar coleta automática de inventário de hardware e software dos sistemas monitorados.

5.4.18. A solução deve implementar arquitetura baseada em agentes executando em endpoints monitorados.

5.4.19. Deve implementar indexação e armazenamento de alertas gerados pelo servidor.

5.5. **PLATAFORMA DE GERENCIAMENTO DE SERVIÇOS DE SEGURANÇA**

5.5.1. A CONTRATADA deverá disponibilizar ao CONTRATANTE acesso a uma plataforma centralizada de gerenciamento, que atuará como camada de orquestração e visibilidade unificada para todos os serviços e disciplinas de segurança da informação previstos neste termo de referência.

5.5.2. A plataforma deverá consolidar os dados provenientes do monitoramento de ativos, gestão de vulnerabilidades, inteligência de ameaças e proteção de endpoints, permitindo uma visão convergente entre a saúde da infraestrutura de tecnologia e a postura de cibersegurança da instituição.

5.5.3. A interface de gerenciamento deve ser baseada em navegador web, possuir capacidades de visualização interativa e permitir a realização de drill-down para análises detalhadas e investigação de eventos específicos em tempo real.

5.5.4. **As capacidades esperadas para a plataforma incluem, no mínimo:**

I - Visualização Unificada e Convergente

II - Centralização de indicadores de diferentes fontes de dados em uma única interface, eliminando silos de informação e proporcionando visibilidade completa da superfície de ataque.

5.5.5. **Dashboards Executivos e Técnicos**

I - Apresentação de cronogramas de atividades recentes, logs de auditoria e status de conformidade com frameworks de segurança da informação.

5.5.6. **Gestão de Desempenho e Acordos de Nível de Serviço (SLA)**

I - Monitoramento analítico da eficiência operacional dos serviços prestados, com exibição de indicadores fundamentais como o Tempo Médio de Detecção (MTTD) e o Tempo Médio de Resposta (MTTR).

II - Painéis específicos para acompanhamento da conformidade de SLA e tendências históricas de incidentes, permitindo a avaliação da evolução da maturidade de segurança ao longo do contrato.

5.5.7. **Orquestração de Resposta e Remediação**

I - Integração dos resultados da gestão de vulnerabilidades, permitindo a identificação, classificação por criticidade e acompanhamento do ciclo de vida de remediação de falhas em ativos de TI.

II - Capacidade de correlacionar eventos de segurança com ações proativas de resposta, visando a redução da exposição cibernética através de um fluxo contínuo de identificação, governança, remediação e monitoramento.

5.5.8. **Detecção de Anomalias e Inteligência Analítica**

5.5.9. **Relatórios Automatizados e Governança**

I - Suporte à avaliação de conformidade regulatória e atendimento a requisitos legais através da documentação histórica de eventos e ações de resposta

tomadas.

5.6. Sistema de Análise de Postura de Segurança da Informação

5.6.1. O Sistema de Análise de Postura de Segurança da Informação, deve permitir:

- I - Cadastro e gestão de soluções de tecnologia implementadas
- II - Cadastro e gestão de soluções de segurança implementadas
- III - Avaliação de conformidade com PPSI Programa de Privacidade e Segurança a Informação
- IV - Avaliação de conformidade com CIS Controls (v8)
- V - Avaliação de conformidade com MITRE ATT&CK
- VI - Avaliação de conformidade com ISO 27001
- VII - Correlação entre frameworks CIS Controls e MITRE ATT&CK
- VIII - Análise e gestão de riscos de segurança
- IX - Planejamento faseado para implementação de controles
- X - Acompanhamento de evolução de postura de segurança
- XI - Geração de relatórios e recomendações baseadas em inteligência de ameaças

5.6.2. A análise contínua de postura de segurança é essencial para a proteção de dados e infraestrutura de TI, deveser permitir:

- I - Avaliação estruturada e contínua de segurança da informação
- II - Identificação de lacunas de segurança baseada em frameworks internacionais
- III - Correlação entre técnicas de ataque (MITRE ATT&CK) e controles de segurança (CIS)
- IV - Priorização de investimentos em segurança baseada em risco
- V - Planejamento faseado de implementação de controles
- VI - Demonstração de conformidade com regulamentações
- VII - Redução de exposição a ataques cibernéticos
- VIII - Melhoria contínua da postura de segurança
- IX - Otimização de recursos de segurança

5.6.3. CADAstro DE SOLUÇÕES DE TECNOLOGIA

- Registro de servidores (quantidade, SO, versão, localização)
- Registro de estações de trabalho (quantidade, SO, versão)
- Registro de dispositivos de rede (firewalls, switches, roteadores, versão)
- Registro de dispositivos móveis (quantidade, tipo, SO)
- Registro de aplicações críticas (nome, versão, responsável)
- Registro de banco de dados (tipo, versão, dados sensíveis)
- Registro de infraestrutura de backup e disaster recovery
- Registro de conectividade e acesso remoto (VPN, RDP, etc.)
- Registro de segmentação de rede

- Importação em massa de dados (Excel, CSV)
- Edição e exclusão de registros
- Histórico de alterações de cada ativo
- Relatório de inventário de tecnologia

5.6.4. CADASTRO DE SOLUÇÕES DE SEGURANÇA

- Registro de antivírus/antimalware (versão, data de atualização, cobertura)
- Registro de firewalls (tipo, versão, regras, localização)
- Registro de IDS/IPS (tipo, versão, assinaturas)
- Registro de SIEM (tipo, versão, retenção de logs)
- Registro de WAF (Web Application Firewall)
- Registro de Acesso Remoto (tipo, versão, protocolo) ex.: VPN/ZTNA
- Registro de autenticação multifator (tipo, cobertura)
- Registro de criptografia de dados (tipo, escopo)
- Registro de backup automatizado (frequência, retenção)
- Registro de DLP (Data Loss Prevention)
- Registro de EDR (Endpoint Detection and Response)
- Registro de SOAR (Security Orchestration, Automation and Response)
- Registro de gerenciamento de identidade e acesso (IAM)
- Registro de outras soluções de segurança
- Status de ativação (ativo/inativo)
- Data de implementação
- Responsável pela solução
- Mapeamento com controles CIS
- Mapeamento com técnicas MITRE
- Edição em massa e histórico de alterações

5.6.5. CADASTRO DE ATIVOS DE TECNOLOGIA

- Classificação de ativos (crítico, importante, padrão)
- Registro de vulnerabilidades conhecidas
- Registro de patches e atualizações
- Histórico de incidentes relacionados
- Relatório de ativos críticos

5.6.6. AVALIAÇÃO DE CONFORMIDADE DO PPSI

- Suporte aos requisitos e diretrizes do Programa de Privacidade e Segurança da Informação
- Avaliação por nível de maturidade e implementação (ex: 0-3 ou 0-5)
- Descrição detalhada de cada diretriz de privacidade e segurança
- Mapeamento automático com processos, políticas e soluções implementadas

- Anexação de evidências de conformidade (documentos, registros e logs)
- Comentários e notas sobre cada requisito avaliado
- Cálculo automático de score de adequação ao PPSI (0-100%)
- Identificação de riscos críticos, gaps e controles prioritários
- Agrupamento por domínios (ex: Governança, Privacidade, Proteção de Dados e Defesa Cibernética)
- Histórico de avaliações e auditorias anteriores
- Comparação temporal da evolução da conformidade
- Relatório de conformidade do PPSI (incluindo status de adequação à LGPD)
- Exportação em PDF e Excel

5.6.7. AVALIAÇÃO DE CONFORMIDADE CIS CONTROLS

- Suporte a 150+ controles CIS v8
- Avaliação por nível de implementação (0-3)
- Descrição detalhada de cada controle
- Mapeamento automático com soluções implementadas
- Anexação de evidências de implementação
- Comentários e notas sobre cada controle
- Cálculo automático de score de conformidade (0-100%)
- Identificação de controles críticos e prioritários
- Agrupamento por categoria de controle
- Histórico de avaliações anteriores
- Comparação temporal de conformidade
- Relatório de conformidade CIS
- Exportação em PDF e Excel

5.6.8. AVALIAÇÃO MITRE ATT&CK

- Suporte a 200+ técnicas MITRE ATT&CK
- Mapeamento com 14 táticas MITRE
- Correlação com soluções de segurança implementadas
- Correlação com controles CIS
- Identificação de técnicas expostas
- Cálculo de cobertura por tática
- Cálculo de cobertura geral
- Visualização em matriz interativa
- Filtros por tática, técnica, plataforma
- Recomendações de mitigação
- Histórico de evolução de cobertura
- Comparação com benchmark do setor
- Relatório de postura MITRE

- Exportação em PDF e Excel

5.6.9. CORRELAÇÃO ENTRE CIS CONTROLS E MITRE ATT&CK

- Mapeamento completo de 150+ controles CIS com 200+ técnicas MITRE
- Visualização em página única correlacionando ambos frameworks
- Identificação de técnicas expostas por controle não implementado
- Análise de lacunas de segurança
- Recomendações de controles prioritários
- Visualização de impacto de cada controle
- Priorização automática de implementação
- Relatório de correlação CIS-MITRE
- Exportação de matriz de correlação

5.6.10. AVALIAÇÃO E GESTÃO DE RISCOS

- Cadastro de riscos identificados
- Classificação de riscos (Técnico, Operacional, Estratégico)
- Avaliação de probabilidade (1-5)
- Avaliação de impacto (1-5)
- Cálculo automático de score de risco (Probabilidade × Impacto)
- Status de risco (Aberto, Mitigado, Aceito, Eliminado)
- Proprietário do risco
- Plano de mitigação
- Matriz de risco interativa (5×5)
- Visualização de riscos por categoria
- Filtros por status e severidade
- Histórico de alterações de risco
- Associação de controles a riscos
- Cálculo de redução de risco por controle
- Relatório de análise de riscos
- Exportação em PDF e Excel

5.6.11. ACOMPANHAMENTO DE EVOLUÇÃO DE POSTURA DE SEGURANÇA

- Dashboard de conformidade geral (0-100%)
- Score por framework (CIS, MITRE, ISO 27001)
- Comparação de scores entre avaliações
- Alertas de tendência negativa
- Relatório de evolução de postura
- KPIs de segurança
- Exportação de gráficos e relatórios

5.7. REQUISITOS TÉCNICOS COMPROVADOS DA PLATAFORMA DE DEFESA CIBERNÉTICA

5.7.1. Os requisitos relacionados nesta seção correspondem a funcionalidades efetivamente comprovadas na Matriz de Comprovação Técnica da plataforma de defesa cibernética, com indicação de documento, página e seção que evidenciam cada item, e integram o escopo mínimo exigível da SOLUÇÃO.

5.7.2. **Arquitetura, implantação e escalabilidade**

5.7.2.1. A SOLUÇÃO deverá ser plataforma unificada de defesa cibernética, operada a partir de console único, que concentre em uma mesma experiência integrada o monitoramento de segurança, a análise de postura, a governança, a gestão de risco, o compliance, a correlação de eventos de segurança (SIEM), a gestão de vulnerabilidades e a inteligência de ameaças, vedada a entrega por meio de ferramentas independentes sem integração entre si.

5.7.2.2. A SOLUÇÃO deverá ser organizada em módulos integrados sob núcleo comum, contemplando no mínimo: operação de segurança em tempo real, priorização de vulnerabilidades por risco, governança de risco e compliance, e inteligência de ameaças, todos acessíveis pelo mesmo console e apoiados na mesma base de dados.

5.7.2.3. A SOLUÇÃO não deverá ser fornecida em modalidade de serviço gerenciado em nuvem.

5.7.2.4. A SOLUÇÃO deverá admitir, alternativamente, implantação em infraestrutura própria do CONTRATANTE, seja local ou em nuvem privada sob sua guarda, por meio de containers, com administração integral da solução pela equipe do CONTRATANTE, de modo a atender requisitos de soberania de dados.

5.7.2.5. Na implantação em infraestrutura própria, a SOLUÇÃO deverá operar sobre componentes de banco de dados relacional e de cache em memória, com containers endurecidos.

5.7.2.6. A SOLUÇÃO deverá possuir mecanismo de alta disponibilidade que a mantenha operante e responsiva ainda que as fontes externas de dados fiquem indisponíveis, mediante sincronização dos dados para base local e entrega por camada de cache.

5.7.2.7. As consultas realizadas pelas telas da SOLUÇÃO deverão ser atendidas a partir da base local ou da camada de cache, de modo que o tempo de resposta ao usuário não dependa da latência ou da disponibilidade das fontes externas no instante da consulta.

5.7.2.8. A SOLUÇÃO deverá ser construída sobre arquitetura preparada para crescimento de volume, com processamento em segundo plano e camada de cache que preservem desempenho e disponibilidade sob alta carga.

5.7.2.9. A documentação técnica da SOLUÇÃO deverá ser fornecida integralmente em português do Brasil.

5.7.3. **Multilocação (multi-tenant) e isolamento de dados**

5.7.3.1. A SOLUÇÃO deverá adotar arquitetura multilocatária (multi-tenant) com isolamento total dos dados entre as organizações atendidas, vedado o compartilhamento de dados entre locatários.

5.7.3.2. Cada organização atendida deverá operar com banco de dados dedicado, de modo que o isolamento seja assegurado na camada de persistência e não apenas por filtro de aplicação.

5.7.3.3. Cada organização atendida deverá operar com instância de cache dedicada, assegurando que os dados em memória também permaneçam segregados por locatário.

5.7.3.4. A SOLUÇÃO deverá oferecer nível de visão consolidada, na forma de locatário virtual ou visão global, que agregue os indicadores de todas as organizações atendidas para a equipe responsável pela operação, sem misturar os dados de cada locatário nas visões individuais.

5.7.3.5. A SOLUÇÃO deverá dispor de função de administração multilocatária, com provisionamento e manutenção das organizações atendidas pela própria interface administrativa.

5.7.3.6. O isolamento de dados por organização deverá integrar os controles de segurança e governança da SOLUÇÃO, e não apenas a sua arquitetura de dados.

5.7.4. **Coleta de telemetria e cobertura de ativos**

5.7.4.1. A SOLUÇÃO deverá realizar coleta de telemetria por agentes nativos para os sistemas operacionais Windows, Linux e macOS.

5.7.4.2. A SOLUÇÃO deverá disponibilizar instaladores dedicados para cada sistema operacional suportado pelos agentes de coleta.

5.7.4.3. A coleta por agentes deverá abranger estações de trabalho e servidores, permitindo detecção em ambos os tipos de ativo.

5.7.4.4. A SOLUÇÃO deverá apresentar painel do parque de agentes em tempo real, discriminando no mínimo os estados ativo, desconectado, nunca conectado e pendente.

5.7.4.5. Para cada agente, a SOLUÇÃO deverá manter e exibir a versão instalada, o sistema operacional e a data e hora do último sinal de atividade.

5.7.4.6. A SOLUÇÃO deverá sinalizar automaticamente os agentes com versão desatualizada.

5.7.4.7. A SOLUÇÃO deverá permitir a exportação do inventário de agentes em formato CSV.

5.7.4.8. A SOLUÇÃO deverá integrar-se, por interface de programação de aplicações, a fontes externas de telemetria e de inteligência, incorporando os dados coletados às suas próprias análises.

5.7.4.9. A SOLUÇÃO deverá incorporar, por integração, métricas de disponibilidade e de capacidade da infraestrutura, convergindo-as com os demais dados para priorização de ações.

5.7.5. **Monitoramento, detecção e correlação de eventos**

5.7.5.1. A SOLUÇÃO deverá centralizar alertas, regras de detecção e técnicas de ataque associadas, com políticas de retenção e rotinas de sincronização automatizadas.

5.7.5.2. A SOLUÇÃO deverá apresentar resumo dos alertas por severidade referente às últimas 24 horas.

5.7.5.3. A SOLUÇÃO deverá identificar automaticamente picos de alertas no período monitorado.

5.7.5.4. A SOLUÇÃO deverá apresentar a evolução temporal dos alertas com análise de tendência em janelas de 7 e de 30 dias.

5.7.5.5. A SOLUÇÃO deverá apresentar ranking das regras de detecção que mais dispararam e dos ativos que mais geram alertas.

5.7.5.6. A SOLUÇÃO deverá correlacionar os alertas por nível ou severidade da regra e identificar automaticamente candidatos a falso positivo, subsidiando o ajuste contínuo das detecções.

5.7.5.7. A SOLUÇÃO deverá consultar os dados em tempo real das fontes integradas e sinalizar automaticamente, por indicador de atualidade, quando uma fonte estiver indisponível ou com dados defasados.

5.7.5.8. A SOLUÇÃO deverá oferecer visão consolidada por ativo, reunindo os últimos alertas, as vulnerabilidades identificadas e as técnicas de ataque associadas ao mesmo ativo.

5.7.5.9. A SOLUÇÃO deverá disponibilizar dados forenses de rede por ativo, contemplando endereços IP, portas, protocolos e geolocalização, apresentados em linha do tempo de atividades.

5.7.5.10. A SOLUÇÃO deverá apresentar fluxo de eventos em tempo real com fila de priorização por classe, controle de prazo por evento e ranking das regras acionadas, permitindo aprofundamento investigativo a partir do próprio fluxo.

5.7.5.11. A SOLUÇÃO deverá dispor de mecanismo de busca e indexação de alto desempenho sobre grandes volumes de eventos.

5.7.5.12. A priorização do fluxo de eventos deverá considerar impacto, urgência e confiança da detecção.

5.7.6. **Cobertura MITRE ATT&CK e maturidade de detecção**

5.7.6.1. A SOLUÇÃO deverá classificar as detecções segundo táticas e técnicas do framework MITRE ATT&CK, apresentando a distribuição resultante.

5.7.6.2. A SOLUÇÃO deverá calcular e apresentar o percentual de cobertura de detecção em relação ao conjunto de técnicas do MITRE ATT&CK Enterprise.

5.7.6.3. A SOLUÇÃO deverá identificar e priorizar as lacunas de detecção nas táticas mais críticas.

5.7.6.4. A SOLUÇÃO deverá apresentar a trajetória do alerta desde a fonte até a conclusão do tratamento, mapeada sobre as táticas do MITRE ATT&CK.

5.7.6.5. As hipóteses de caça a ameaças deverão ser associadas a táticas e técnicas do MITRE ATT&CK.

5.7.6.6. A SOLUÇÃO deverá apresentar avaliação de conformidade técnica da configuração dos ativos frente a linhas de base de segurança reconhecidas, com pontuação por ativo.

5.7.7. **Gestão de vulnerabilidades**

5.7.7.1. A SOLUÇÃO deverá apresentar a distribuição da base de vulnerabilidades por faixa de criticidade CVSS, contemplando crítica, alta, média e baixa, com histograma por pontuação e aprofundamento por severidade.

5.7.7.2. A SOLUÇÃO deverá relacionar as vulnerabilidades mais críticas identificadas com a respectiva pontuação CVSS e a quantidade de ativos afetados.

5.7.7.3. A SOLUÇÃO deverá cruzar a base de vulnerabilidades com catálogo público de vulnerabilidades exploradas ativamente, destacando os itens nele listados.

5.7.7.4. A SOLUÇÃO deverá apresentar ranking dos ativos mais vulneráveis, informando a contagem de vulnerabilidades críticas e altas, o sistema operacional e a pontuação de risco de cada ativo.

5.7.7.5. A SOLUÇÃO deverá medir a cobertura de correções frente à meta estabelecida, segmentando por sistema operacional e por ativo, e rastreando os ativos críticos ainda sem correção.

5.7.7.6. A SOLUÇÃO deverá apresentar gráfico de redução acumulada das

vulnerabilidades críticas abertas e fechadas ao longo do tempo, com linha de previsão, meta de resolução e apuração das novas e das fechadas nos últimos 7 dias.

5.7.7.7. A SOLUÇÃO deverá controlar prazos de remediação por severidade, apurando o percentual de conformidade e o status individual de cada vulnerabilidade.

5.7.7.8. A SOLUÇÃO deverá priorizar automaticamente as violações de prazo de remediação, apresentando-as em fila de ação.

5.7.7.9. A SOLUÇÃO deverá apresentar a tendência de 30 dias do cumprimento dos prazos de remediação.

5.7.7.10. A SOLUÇÃO deverá apresentar filas de ação ordenadas por impacto, orientando a sequência de tratamento.

5.7.7.11. As vulnerabilidades identificadas deverão estar acessíveis também pela visão individual do ativo, associadas aos respectivos alertas e técnicas de ataque.

5.7.8. **Governança de risco e resposta a incidentes**

5.7.8.1. A SOLUÇÃO deverá apresentar matriz de risco cruzando probabilidade e impacto, com codificação por cores e plotagem dos incidentes conforme a severidade.

5.7.8.2. A SOLUÇÃO deverá destacar, em fila prioritária, os incidentes de maior risco apurado.

5.7.8.3. A SOLUÇÃO deverá realizar análise de causa raiz dos incidentes, com agrupamento por causa, ranking de frequência, identificação da severidade dominante por causa e tendência ao longo do tempo.

5.7.8.4. A SOLUÇÃO deverá apresentar recomendações de ações preventivas decorrentes da análise de causa raiz.

5.7.8.5. A SOLUÇÃO deverá controlar prazos de resposta a incidentes por severidade, apresentando o status individual de cada incidente, a conformidade consolidada e a tendência do indicador.

5.7.8.6. A SOLUÇÃO deverá apurar o tempo médio de resposta agrupado por categoria de incidente, com média, percentual, distribuição de severidade, linha de referência da meta e destaque dos melhores e piores desempenhos.

5.7.8.7. A SOLUÇÃO deverá calcular e apresentar pontuação de risco consolidada da postura de segurança da organização.

5.7.8.8. A SOLUÇÃO deverá apresentar análise de conformidade do ambiente e apoiar a adequação a frameworks e normas de segurança da informação.

5.7.8.9. A priorização apresentada pela SOLUÇÃO deverá considerar o impacto no negócio.

5.7.8.10. A SOLUÇÃO deverá registrar e acompanhar a resposta a incidentes de segurança até a conclusão do tratamento.

5.7.9. **Indicadores, análise e relatórios**

5.7.9.1. A SOLUÇÃO deverá apresentar indicadores executivos no topo de cada tela de análise.

5.7.9.2. A SOLUÇÃO deverá gerar insights executivos com priorização automática, indicando os pontos que exigem atenção imediata.

5.7.9.3. A SOLUÇÃO deverá permitir aprofundamento investigativo do panorama consolidado até o detalhe do registro individual em poucos cliques.

5.7.9.4. A SOLUÇÃO deverá disponibilizar gráficos interativos de evolução e de tendência.

5.7.9.5. A SOLUÇÃO deverá apresentar filas de ação priorizadas nas telas de análise, com indicação do que deve ser tratado primeiro.

5.7.9.6. A SOLUÇÃO deverá disponibilizar relatórios em tempo real e relatórios históricos.

5.7.9.7. A SOLUÇÃO deverá permitir a exportação dos dados apresentados em formato CSV.

5.7.9.8. A SOLUÇÃO deverá apurar os indicadores de tempo médio de reconhecimento, de detecção e de resposta frente às metas de nível de serviço estabelecidas.

5.7.9.9. A SOLUÇÃO deverá apurar taxa de acurácia, volume de alertas tratados, quantidade de analistas ativos e conformidade frente às metas, com tendência de 30 dias.

5.7.9.10. A SOLUÇÃO deverá apresentar indicadores de desempenho por analista, permitindo a gestão da equipe de operação por dados.

5.7.9.11. A SOLUÇÃO deverá dispor de painel executivo consolidando superfície de ataque, pontuação de risco e incidentes críticos priorizados.

5.7.9.12. A SOLUÇÃO deverá fornecer métricas executivas que permitam comprovar a postura de segurança à alta administração.

5.7.10. **Controle de acesso, segurança e auditoria**

5.7.10.1. A autenticação dos usuários da SOLUÇÃO deverá ser realizada por token assinado.

5.7.10.2. A SOLUÇÃO deverá exigir segundo fator de autenticação baseado em senha de uso único por tempo, de forma obrigatória para todos os usuários.

5.7.10.3. A SOLUÇÃO deverá implementar controle de acesso baseado em papéis, com perfis distintos de administração e de uso e possibilidade de perfil com acesso à visão global.

5.7.10.4. A SOLUÇÃO deverá manter gestão das sessões de usuário, permitindo o seu controle e encerramento.

5.7.10.5. A SOLUÇÃO deverá manter trilha de auditoria completa de todas as ações praticadas pelos usuários.

5.7.10.6. A SOLUÇÃO deverá aplicar cabeçalhos de segurança nas respostas da aplicação web.

5.7.10.7. A SOLUÇÃO deverá permitir a gestão de usuários, papéis e permissões pela própria interface de administração.

5.7.10.8. Os controles de autenticação, autorização e auditoria deverão integrar a arquitetura da SOLUÇÃO como configuração padrão, e não como componente opcional.

5.7.11. **Sincronização, retenção e administração**

5.7.11.1. A SOLUÇÃO deverá dispor de agendador de rotinas em segundo plano que sincronize agentes, alertas, vulnerabilidades e métricas em intervalos otimizados, sem intervenção manual.

5.7.11.2. A SOLUÇÃO deverá monitorar e exibir o status das rotinas de sincronização.

5.7.11.3. A SOLUÇÃO deverá permitir a configuração de políticas de retenção de dados, com rotina automatizada de limpeza dos dados que excederem o período definido.

5.7.11.4. A SOLUÇÃO deverá permitir a gestão dos agentes de coleta e das fontes de dados pela própria interface de administração.

5.7.11.5. A SOLUÇÃO deverá utilizar cache em duas camadas para assegurar desempenho e disponibilidade das consultas.

5.7.11.6. A SOLUÇÃO deverá sinalizar automaticamente, por indicador próprio, a indisponibilidade ou a defasagem dos dados de cada fonte integrada.

6. INDICADORES DE NÍVEIS DE SERVIÇO E NÍVEIS MÍNIMOS DE SERVIÇO (INS/NMS)

6.1. Diretrizes Gerais

6.1.1. A CONTRATADA deverá garantir a prestação dos serviços com base em indicadores objetivos de desempenho, mensurados continuamente e vinculados a níveis mínimos de serviço (NMS, conforme diretrizes do modelo de contratação de TIC do SISP.

6.1.2. Os indicadores definidos nesta seção terão caráter obrigatório e serão utilizados para:

- a) aferição da qualidade dos serviços prestados;
- b) verificação do cumprimento contratual;
- c) aplicação de penalidades e ajustes financeiros;
- d) suporte à governança e à tomada de decisão da CONTRATANTE.

6.1.3. Todos os indicadores deverão ser mensurados de forma automatizada, com base em dados coletados pela própria plataforma ou por mecanismos independentes de monitoramento, garantindo rastreabilidade, auditabilidade e reprodutibilidade dos resultados.

6.1.4. A CONTRATADA deverá disponibilizar dashboards e relatórios contendo a apuração dos indicadores, com atualização em tempo real ou periodicidade mínima diária.

6.2. Os indicadores relacionados a seguir tem relação direta a estas especificações e estão detalhados no Apêndice V, do ETP 6/2026:

- I. INS11 - Tempo Médio de Resposta Autônoma (MTTA-AI)
- II. INS 12 - Taxa de Resolução Autônoma de Incidentes
- III. INS 13 — Disponibilidade da Plataforma da CONTRATADA

6.3. Consolidação e Apuração dos Indicadores

6.3.1. A apuração dos indicadores será realizada mensalmente.

6.3.2. A CONTRATADA deverá apresentar relatório consolidado contendo:

- a) valor apurado de cada indicador;
- b) memória de cálculo detalhada;
- c) eventos considerados e excluídos;
- d) evidências técnicas associadas;

6.3.3. A CONTRATANTE poderá auditar, a qualquer tempo, os dados utilizados

na apuração dos indicadores.

6.4. Disposições Complementares

6.4.1. O não atingimento das metas estabelecidas implicará aplicação de penalidades contratuais, conforme tabela de faixas de desempenho a ser definida em instrumento específico.

6.4.2. Disposições Complementares

6.4.3. Todos os dados utilizados na mensuração dos indicadores são de propriedade da CONTRATANTE.

6.4.4. A CONTRATADA deverá garantir a integridade, disponibilidade e rastreabilidade dos dados de medição por todo o período contratual.

6.4.5. A CONTRATADA deverá disponibilizar acesso à CONTRATANTE para consulta em tempo real dos indicadores.

7. PROVA DE CONCEITO - POC

7.1. Os requisitos da prova de conceito estão separados por ferramenta, na mesma ordem das seções deste Apêndice. A LICITANTE deverá demonstrar cada requisito e assinalar Sim ou Não, registrando na coluna Observação a evidência apresentada.

7.2. Solução de Gerenciamento de Serviços de TIC (ITSM)

7.2.1. A Tabela a seguir apresenta a lista de requisitos da Solução de Gerenciamento de Serviços de TIC que deverão ser demonstrados pela LICITANTE, obrigatoriamente de forma presencial na sede do ITI durante a realização da prova de conceito:

Requisitos da Prova de Conceito			Conformidade de Atendimento	
Nº	Tipo	Requisito	Sim	Não
1	Gestão de Serviços e Ativos	Os serviços cadastrados devem permitir o vínculo com ativos suportados.		
2	Gestão de Serviços e Ativos	Os serviços cadastrados devem permitir o vínculo do Cliente demandante do serviço.		
4	Gestão de Serviços e Ativos	Os acordos de nível de serviço devem ser vinculados ao serviço e exibidos no próprio dossiê do serviço, de modo que o analista tenha acesso imediato a prazos e metas durante o atendimento.		
5	Gestão de Serviços e Ativos	O cadastro do serviço deve permitir o vínculo com contrato.		
6	Gestão de Serviços e Ativos	Deve possuir relatório de ativos vinculados a serviços.		
7	Gestão de Serviços e Ativos	O cadastro do ativo e o cadastro do serviço devem permitir o vínculo com contrato, inclusive para serviços gerenciados.		

8	Gestão de Serviços e Ativos	O cadastro do ativo deve conter nome, tipo, fabricante, modelo, número de série, contrato, localização e etiqueta de patrimônio, e deve permitir a geração de etiqueta com QR Code que dê acesso direto à abertura de chamado para aquele ativo.		
9	Gestão de Incidentes e Requisições	Deve apresentar os indicadores do próprio serviço: total de chamados, incidentes, requisições, chamados abertos, prazos estourados e tempo médio de solução.		
10	Gestão de Incidentes e Requisições	A solução deve notificar requerentes, analistas e observadores quando o chamado ultrapassar o percentual do prazo de solução definido pela Gestão da Instituição, com verificação a cada 15 minutos e percentual parametrizável, adotado 95% como padrão.		
11	Gestão de Incidentes e Requisições	A solução deve enviar notificação diária aos administradores com a relação dos chamados pendentes há mais tempo que o período definido pela Gestão da Instituição, informando os dias de pendência e o responsável por cada chamado.		
12	Gestão de Incidentes e Requisições	A solução deve encerrar automaticamente os chamados pendentes há mais tempo que o período definido pela Gestão da Instituição, com a rotina desligada por padrão até que a Gestão defina o prazo.		
14	Gestão de Incidentes e Requisições	A solução deve possuir painel nativo do processo de gestão de incidentes contendo, no mínimo, volume de incidentes registrados, volume de incidentes encerrados, tempo médio de solução, tempo médio de atribuição, satisfação média e incidentes solucionados sem uso de artigo da base de conhecimento.		
16	Gestão de Incidentes e Requisições	A solução deve possuir painel de desempenho da equipe na gestão de requisições.		
17	Gestão de Problemas	A solução deve permitir a criação do Relatório de Causa Raiz dentro do registro do problema, com estado próprio, separado do status do problema.		
18	Gestão de Problemas	O Relatório de Causa Raiz deve possuir campo para o registro técnico da ocorrência, de preenchimento obrigatório para o encerramento.		

19	Gestão de Problemas	O Relatório de Causa Raiz deve possuir campo para o registro da solução de contorno, de preenchimento obrigatório para o encerramento.		
20	Gestão de Problemas	O Relatório de Causa Raiz deve possuir campo para o registro da evidência que identificou a causa raiz, de preenchimento obrigatório para o encerramento.		
21	Gestão de Problemas	O Relatório de Causa Raiz deve possuir campo para o plano de ação contra a recorrência do problema em produção, de preenchimento obrigatório para o encerramento.		
22	Gestão de Problemas	O problema somente poderá ser encerrado com o Relatório de Causa Raiz já encerrado, com a trava aplicada no servidor e não apenas na interface.		
23	Gestão de Problemas	O Relatório de Causa Raiz somente poderá ser encerrado com todos os seus campos preenchidos, e a mensagem de recusa deve nomear os campos que faltam.		
24	Gestão de Mudanças	A solução deve possuir formulário de registro de mudanças contendo plano de implantação, plano de reversão, comitê de aprovação e janela planejada.		
25	Gestão de Mudanças	A solução deve permitir a tipificação da mudança entre Normal, Pré-aprovada, Emergencial e Planejada.		
26	Gestão de Mudanças	Para cada item de configuração impactado pela mudança, a solução deve permitir o registro descritivo do impacto numa visão otimista e do impacto numa visão pessimista, mantidos no vínculo entre a mudança e o IC, de modo que a mesma mudança possa ser avaliada de forma distinta em cada ativo.		
27	Aprovações e Notificações Automatizadas	A solução deve enviar periodicamente, por e-mail, relatório de desempenho da equipe ao gestor marcado no cadastro da própria equipe, recaindo nos administradores quando não houver gestor marcado.		
28	Aprovações e Notificações Automatizadas	A solução deve enviar por e-mail aos responsáveis pelas unidades de negócio o desempenho da entrega de serviços em sua unidade, contendo volume, resolvidos, prazos estourados e satisfação.		

29	Aprovações e Notificações Automatizadas	A solução deve enviar e-mail diário aos usuários com aprovações pendentes, limitado a um lembrete por aprovador por dia.		
30	Aprovações e Notificações Automatizadas	A solução deve permitir ao administrador estipular o prazo máximo, em dias, que o chamado pode permanecer aguardando aprovação e, esgotado o prazo, encerrar o chamado por não aprovação.		
31	Aprovações e Notificações Automatizadas	A solução deve notificar diariamente os usuários que ainda possuam pendências de aprovação em chamados abertos.		
32	Aprovações e Notificações Automatizadas	A solução deve permitir a aprovação ou a reprovação do chamado diretamente pelo e-mail, por link de uso único por aprovador, sem exigir acesso à ferramenta e sem que o link sirva uma segunda vez.		
33	Relatórios e Dashboards	A solução deve possuir módulo de relatórios e painéis para a tomada de decisão da Gestão, com exportação em PDF e painéis executivo, tático e operacional.		
34	Relatórios e Dashboards	A solução deve produzir indicadores a partir de coleta em formatos abertos, permitindo ao administrador cadastrar a fonte em endpoint XML ou JSON, com autenticação opcional, informar os caminhos do documento, conferir o valor lido em pré-visualização antes de salvar e agendar a coleta, tudo sem desenvolvimento.		
35	Relatórios e Dashboards	A solução deve permitir a vinculação entre indicadores e relatórios, com o relatório montado pelo administrador bloco a bloco, atualização automática da leitura no intervalo definido e alternância entre os níveis de detalhamento global, parcial e individual sem recarregar a página.		
36	Relatórios e Dashboards	A solução deve permitir ao administrador configurar gráficos comparativos com visualização web, contemplando ao menos oito tipos de gráfico, eixo por rótulo, por agrupamento ou por tempo, até oito séries com cor própria, empilhamento, legenda, rótulo de valor e linha de meta, com prévia redesenhada a cada alteração.		

37	Relatórios e Dashboards	A solução deve manter o histórico de cada indicador por rodada de coleta, com meta e sentido definidos, apresentar a evolução no tempo com a linha de meta e sinalizar, em cada leitura, o desvio em relação à meta.		
38	Relatórios e Dashboards	A solução deve possuir painel de análise de performance por Grupo contendo requisições abertas, encerradas e solucionadas por dia, incidentes abertos, encerrados e solucionados por dia, as dez maiores categorias, os chamados fora do prazo, o total de chamados, os integrantes do grupo e a divisão entre dentro e fora do prazo.		
39	Relatórios e Dashboards	A solução deve possuir relatório de desempenho por analista, com a quantidade de chamados atendidos, resolvidos, o tempo médio de atendimento e a aderência ao acordo de nível de serviço.		
40	Autenticação e Integrações de Comunicação	A solução deve permitir, inclusive em ambiente de nuvem, a autenticação de usuários via SSO de forma segura.		
43	Autenticação e Integrações de Comunicação	A solução deve permitir a autenticação por OAuth2 com Google, Microsoft, cabendo ao CONTRATANTE registrar o aplicativo e informar o identificador e o segredo do cliente.		
45	Autenticação e Integrações de Comunicação	A solução deve permitir ao administrador definir os domínios válidos para a autenticação por OAuth, com aceite de subdomínio, e deve recusar a ativação da criação automática de usuários sem lista de domínios definida.		
46	Autenticação e Integrações de Comunicação	A solução deve bloquear todo acesso não configurado pelo administrador, mantendo o provedor desligado por padrão, não iniciando o fluxo sem credencial cadastrada e recusando e-mail desconhecido quando a criação automática estiver desligada.		
48	Autenticação e Integrações de Comunicação	A solução deve enviar notificações de atualização de chamado por WhatsApp, pela Cloud API da Meta, com ou sem uso de template, cabendo ao CONTRATANTE o número comercial verificado, o template aprovado e o token de acesso.		

49	Autenticação e Integrações de Comunicação	A solução deve enviar notificações de atualização de chamado via Telegram, configurável na tela com token de bot e chat de destino e com teste de conexão.		
50	Autenticação e Integrações de Comunicação	A solução deve enviar notificações de atualização de chamado via Microsoft Teams, por webhook de entrada, com roteamento por equipe.		
51	Monitoria	A SOLUÇÃO deve disponibilizar painéis de monitoramento de status de chamado para monitoria e acompanhamento, com indicadores e alertas, permitindo interação direto pela pagina de monitoria.		
52	Relatórios	Personalização com logo, período de SLA, INS, relatório completos gerados em PDF.		

7.3. Plataforma de Monitoramento Avançado com IA para Operações de TI (AIOps)

Requisitos da Prova de Conceito			Conformidade de Atendimento	
Nº	Tipo	Requisito	Sim	Não
53	Descoberta automática	Descobrir ativo (VM/Container) automaticamente		
54	Discovery em tempo real	Identificar ativo ao ser criado		
55	Mapa de dependência	Construir relação entre app, serviço e infra		
56	Identificação de criticidade	Classificar ativo crítico		
57	Monitoramento de aplicação	Coletar métricas (tempo resposta, erro)		
58	Distributed tracing	Rastrear transação ponta a ponta		
59	Deteção de anomalia	Detectar degradação sem threshold manual		
60	Correlação de eventos	Agrupar eventos relacionados		
61	Identificação causa raiz	Identificar origem da falha		
62	Criação automática de incidente	Evento gera incidente automaticamente		
63	Associação com CMDB	Relacionar incidente ao ativo		

64	Análise com base histórica	Correlacionar com eventos anteriores		
65	Base de conhecimento	Correlacionar com eventos anteriores		
66	Execução automática	Executar playbook de correção		
67	Remediação autônoma	Resolver incidente sem intervenção humana		
68	Ajuste preditivo	Antecipar degradação futura		
69	Atualização do estado	Atualizar status após correção		
70	Visão unificada	Navegar entre aplicação, evento e infra		
71	Integração cloud/on-prem	Navegar entre aplicação, evento e infra		
72	Aprendizado contínuo	IA melhora após execução		
72.1	Topologia física e lógica	Apresentar, no mesmo grafo de dependências, ativo de armazenamento, empilhamento de comutadores e componente de nuvem pública		
72.2	Agente sem porta em escuta	Demonstrar que o componente instalado nos ativos monitorados não mantém porta de serviço em escuta		
72.3	Reconciliação de inventário	Descobrir o mesmo ativo por dois métodos distintos e consolidá-lo em um único item de configuração, com registro da fonte que prevaleceu		
72.4	Triagem de eventos	Demonstrar o registro distinto entre a caracterização do evento e a decisão de acionamento, com apuração da taxa de supressão por fonte		
72.5	Autonomia graduada	Configurar a mesma ação como automática em um ambiente e sujeita a aprovação em outro, sem desenvolvimento		
72.6	Auditabilidade da decisão	Reconstituir integralmente uma decisão automatizada a partir dos dados persistidos (entrada, raciocínio, ação, parâmetros, resultado e modelo)		

7.4. Plataforma de Orquestração de Conhecimento com LLMs em Low-Code e LLMOps

Requisitos da Prova de Conceito			Conformidade de Atendimento	
Nº	Tipo	Requisito	Sim	Não
73	Geração de resposta com RAG	O sistema deverá responder a consulta utilizando base de conhecimento previamente ingerida, por meio de mecanismo RAG (Retrieval-Augmented Generation)		
71	Segurança contra prompt injection	O sistema deverá identificar e bloquear tentativas de manipulação do modelo por meio de prompts maliciosos		
75	Orquestração multi-LLM	A plataforma deverá executar requisição utilizando modelo e no mesmo fluxo utilizar outro modelo para sequência da tarefa		
76	Execução de fluxo automatizado com IA	O sistema deverá executar fluxo de trabalho definido em linguagem natural, envolvendo múltiplas etapas automatizadas com uso de IA		
77	Geração automatizada de documento técnico	O sistema deverá gerar documento técnico estruturado a partir de dados reais (ex.: incidente, logs ou métricas)		
77.1	Consulta em linguagem natural	Formular consulta analítica em linguagem natural sobre base conectada, exibindo a consulta estruturada gerada antes da execução		
77.2	Proteção da base de dados	Demonstrar o bloqueio de comando de manipulação de dados em consulta gerada e a recusa de credencial com privilégio de escrita		
77.3	Cruzamento federado	Cruzar dados de duas fontes distintas sem persistência intermediária dos dados consultados		
77.4	Auditoria de consultas	Exibir o registro auditável da consulta realizada, com usuário, fonte, consulta executada e custo apurado		

7.5. Plataforma de Segurança e Governança da Informação

Requisitos da Prova de Conceito			Conformidade de Atendimento	
Nº	Tipo	Requisito	Sim	Não
78	Análise de Postura de Segurança da Informação	O Sistema de Análise de Postura de Segurança da Informação, deve permitir:		

79	Análise de Postura de Segurança da Informação	Avaliação de conformidade com Programa de Privacidade e Segurança a Informação (PPSI)		
80	Análise de Postura de Segurança da Informação	Avaliação de conformidade com CIS Controls (v8).		
81	Análise de Postura de Segurança da Informação	Avaliação de conformidade com MITRE ATT&CK.		
82	Análise de Postura de Segurança da Informação	Avaliação de conformidade com ISO 27001.		
83	Análise de Postura de Segurança da Informação	Correlação entre frameworks CIS Controls e MITRE ATT&CK.		
84	Análise de Postura de Segurança da Informação	Análise e gestão de riscos de segurança.		
85	Análise de Postura de Segurança da Informação	Planejamento faseado para implementação de controles.		
86	Análise de Postura de Segurança da Informação	Acompanhamento de evolução de postura de segurança.		
87	Análise de Postura de Segurança da Informação	Geração de relatórios e recomendações baseadas em inteligência de ameaças.		



Documento assinado eletronicamente por **Rafael de Lima Ramos, Coordenador(a)**, em 01/09/2026, às 11:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Alysson Marques, Coordenador-Geral**, em 01/09/2026, às 11:37, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0811325** e o código CRC **522EF012**.