

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 (Arbitria 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