

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		
		DB-02	Suporte a ETL
		DB-03	Segurança de Dados Críticos
3.5	Conectividade e Comunicação	CC-01	Administração de Ativos de Rede
		CC-02	Gerenciamento de Redes Lógicas
		CC-03	Suporte a Links e Interconexão (WAN/VPN)
3.6	Segurança de TIC	SG-01	Operação do SOC (Security Operations Center)
		SG-02	Gerenciamento de Segurança de Perímetro
		SG-03	Gestão de Credenciais e Acessos
		SG-04	Tratamento de Vulnerabilidades
3.7	Monitoramento de Serviços de TI	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 enlaces, 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 (Threat Intelligence)	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